Techno Security & Digital Forensics Conference

June 3-6, 2018 | Myrtle Beach, SC, USA

Sneak Peek of Confirmed Sessions

(As of February 28, 2018 – the full program will be available by mid-March)

Advanced Analysis Techniques for Mobile Device Evidence: Linux, Python Scripting and Physical Analyzer

As mobile devices become more complicated to gain access to in a forensic manner, automated tools can only do so much. With 88 percent of devices worldwide running Android, there is no easy solution to ensure that examiners can extract data from each of these devices in criminal and civil investigations. During this highly interactive session, attendees will learn the importance of understanding advanced concepts and see examples of how to use Linux and Python Scripting, coupled with the advanced capabilities of Physical Analyzer to acquire and analyze the most relevant data stored on flash memory.

Apple Search Warrants - What to Request and What to Do with What You Receive

With more user data stored on Apple's corporate servers, investigators need to know how to submit a search warrant request to Apple and how to deal with the data they receive back. This session will prepare investigators for how to submit this type of search warrant and what to expect in return. It will also cover how to identify encrypted results, and what can be done to fully extract the contents of the data submitted.

Auditing SQL Server in Every Way Possible

Microsoft SQL Server is in just about every enterprise and government organization in the world and it is trusted to store and serve up even the most sensitive of data. As a result, Microsoft has instrumented SQL Server in such a way that you can audit just about every action a user performs, whether it's changing data, reading data, or manipulating the structure of the data itself. In this session, we'll show you all the places you can turn the knobs and flip the switches in order to audit what you need to and give you some tips into getting that info into downstream systems like an SIEM. We'll also cover if a certain feature has a SQL Server version or edition restriction, so you can determine what you can do with your current technology investment.

Big Forensics – Investigating Very Large Organizations

Digital forensic processing of very large organizations (thousands of nodes) offers some significant challenges when compared to traditional computer forensics. Hence, the term "Big Forensics." These types of investigations entail diverse configurations, operating systems, applications, connectivity, hardware, and components. The sheer volume of devices and data may be beyond investigator's resources. Information that may be of evidentiary interest. Increasingly, because networks may be distributed across multiple jurisdictions, only portions or segments of the data may be readily accessible to investigators in the jurisdiction(s) where the crime occurred. This session will introduce two new technologies to investigate large organizations: File Toolkit for Selective Analysis & Reconstruction (File TSAR), and Devlan (Digital Evidence from Large Networks).

Brains Over Brawn: Intelligent Password Recovery

Attendees will leave this session with new ideas that can immediately be applied to their password cracking needs ranging from recovery of password-protected documents needed for forensics, incident response, law enforcement, and legal cases to improving password compliance in large organizations. We will share our experience running the DEFCON password cracking contest "Crack Me If You Can", our security R&D work for DARPA and for the Carnegie Mellon University CyLab Usable Privacy and Security Laboratory. The session will include numerous real-world examples, and attendees will leave with new cracking ideas that will be immediately beneficial to your password cracking efforts.

Can Machine Learning Really Help an Investigation?

It is predicted that there will be over 20 billion connected devices by 2020 – and that doesn't include over five billion smartphones. Add to that volume the amount of data people are using with their choice of over five million applications, and you can better understand the terabytes and petabytes of data you have to examine in larger cases. Can artificial intelligence in examination tools help you narrow results faster? In this session, we'll discuss the opportunities in machine learning and artificial intelligence for digital forensics. We'll explore teaching software context to find relevant results and prioritize key evidence. You'll learn more about how to integrate these new technologies into your workflow.

Case Study: ModPOS vs RawPOS - A Nerd's-Eye View of Two Malware Frameworks

Although merchants and retailers have been implementing more secure technologies within their payment environments, such as Chip and PIN and Point to Point Encryption, they continue to be targeted by cyber criminals' intent on stealing payment card data. Popular tools used by hackers in these types of breaches include memory-scraping malware such as RawPOS and ModPOS. During this session, we'll provide an overview of these two malware variants, exploring the similarities and differences between them. We'll also discuss forensic artifacts and analysis techniques useful in payment card breach investigations.

Cellular Technology, Mapping, and Analysis: An Introduction into the Technology of Cellular Records and How They Can Be Used in Investigations

This session will provide an in-depth look into cellular networks and call detail records (CDR's) from any cell phone provider. We'll share how to understand the information, how to use the information and why it is critical to your investigations. You'll leave learning the basics of mapping CDRs, how to use advanced reports such as PCMD, RTT, True Call, & EVDO to obtain a more accurate location, how cellular networks communicate with cell phones and more.

Cloud Leaks or Data Breach? Flying Blind in the Clouds!

Are we Flying Blind in the Clouds? 3rd Party Cloud Leaks or data Breach? IT Depends! In this session, we will discuss the rise in cloud leaks and "potential" data breaches. We will share current examples, including types of customer data that have been exposed and the root causes of these cloud leaks. We will also discuss the importance of establishing baselines and monitoring for changes. Finally, we will review the importance of security specific contract language for third parties and a few of the challenges surrounding incident response.

Container Fundamentals with Security Considerations

Container technology realizes the concept of Platform as a Service (PaaS) in cloud computing and standardizes the packaging and deployment of an application and the runtime environment into a repeatable and portable process. The agility in application lifecycle management introduced by containers is compelling and the adoption in the IT industry has been overwhelming and rather aggressive. While the technology is exciting and appears promising, the benefits however should not and need not come at the cost of IT security. What is a container? Why do we care? How it is built? What are the security ramifications? These are all important topics that will be addressed. This session will walk through a process and highlight essential operations and security considerations for architecting, networking, creating, deploying and managing container solutions.

Cybersecurity and Risk Management

Cybersecurity and risk management cybersecurity decisions should be driven from a shared understanding of your organization's assets, threats, and vulnerabilities so that security investments address the most significant risks. Cybersecurity operations, risk management, financial impact realizations as well as investing in the workforce's skills to sustain a hardened security posture are all important to enterprise security. Creating a security strategy that ensures proactive response to an evolving threat landscape is a challenge this session will help organizations achieve success in. In this session we'll share an overview of different cybersecurity controls frameworks (i.e., NIST, ISO, TSC, etc.) and the elements of a cybersecurity risk management program.

Deep Learning Techniques for Detecting Child Pornography in Videos

Current solutions for detecting child pornography in video often rely upon representative key frame image captures that the analyst must manually review. While this method is an improvement over having to view an entire video, it is still time consuming and does not significantly reduce the workload of computer forensic analysts. This session will introduce Advanced Learning Techniques for Detecting Contraband Video, that detect nudity in an image using the ability to detect skin tones and by advanced machine learning techniques that can identify nudity based on connected regions containing skin tone and the relative positions and size; and detect children in a video by exploiting the temporal dimension and using 3-D reconstruction of the subject and extracting features in 3-D that can identify children. This session will also introduce DeepPatrol, a software tool for investigating child pornography cases that will be designed to fit into typical law enforcement investigation workflows.

Don't Let the Hunter Become the Hunted – Protect Your Online Research Network Intelligently

Online research of publicly accessible websites is a source for a practically infinite amount of data. But who knows what sorts of malicious software (malware) is lurking on the other side of every link you click. A malware infection in your research lab’s network can have devastating effects for your organization, ranging from data theft and leakage, ransomware infections, or simply destruction of your data and equipment. If your data is stolen and leaked to the wrong people, it maybe you that is being investigated by your targets! This session will discuss the malware risks you are exposed to when doing online research as well as some cutting edge new ways to protect your network from online malware threats.

Drone Forensics 101: Extracting and Examining Data from Drones

Drones are quickly becoming a major concern for law enforcement agencies around the globe. They have been used to transport contraband across borders, into prisons, and drop propaganda at NFL games. This session will cover forensic concepts, techniques and challenges for extracting and examining data from drones. We’ll also cover sources of drone data, some of the extraction processes, challenges with the data and extracting it, and current capabilities.

Ensuing the Admissibility of Cloud Evidence

This panel discussion will address the relevance of data to solve cases and how it has created new challenges for legally acquiring data and evidence using credentials obtained from mobile devices and for recovering items that may have been deleted from the phone but can be recovered from the cloud. This session will address: When to ask for consent and how to mitigate risk; Under what circumstances is a warrant required; and Examples on how to construct a warrant that aligns with mobile extraction.

Forensic Analyses of Audio, Acoustic, and Video Evidence

Audio, acoustics, voice and video evidence are common in civil and criminal litigation throughout all state and Federal courts. Often such evidence is extracted from a computer or mobile device. All parties must at least be generally familiar with what can (and cannot) be done forensically and legally with such evidence. Authenticity analyses forensically determine if the audio or video evidence is legally trustworthy (admissible), or whether it has been tampered or fabricated in any way (inadmissible). Digital signal processing (enhancement) makes the audio more audible/intelligible, or the video clearer. Photogrammetry allows determination of heights of suspects, etc. Aural-acoustic-spectrography is the forensic comparison of 2 voice samples ("known" vis-a-vis "unknown") based on scientific principles well established in the speech and hearing sciences to determine the identity of a speaker. In this session, you'll learn generally what can and cannot be done, whether you're the proponent or opponent of the evidence, and whether a case needs a consulting, rebuttal or testifying expert witness.

Going Dark: Impact to Law Enforcement and the Intelligence Community and Threat Mitigation

The public and private sectors face a growing national security concern resulting from the ability of criminals, terrorists, and state actors to obfuscate their activities by going dark through encryption or other means. Rapidly evolving technological advancements impede the ability of law enforcement and the Intelligence Community to collect and analyze information critical to thwarting potential threats. At the same time, strong encryption ensures digital communications are protected for secure commerce and trade, strengthens cybersecurity, and safeguards private information, national security, and the global economy. In this session, we'll explore the opportunities and challenges law enforcement and the Intelligence Community face in light of the going dark problem. We'll also share the findings of a team of public and private sector analysts focused on the "going dark" problem and its attempt to collectively address the national security concerns resulting from barriers to data collection.

How Cyber Criminals Shop: An Introduction to Darknet Markets

They have innocent-sounding names like AlphaBay, Europol, and Dream Marketplace. But inside these "hidden" sites cybercriminals gather to buy and sell, connect with other cybercriminals, and develop ideas that will enhance their criminal enterprises. While law enforcement has been able to successfully take down some of the higher profile darknet markets, another market usually quickly rises to take its place. Attendees will be introduced to the types of crimes that are most commonly conducted via marketplaces and which are frowned upon or forbidden outright. The session will explain common darknet market characteristics and operational philosophies. In addition, this session will discuss the important role that cryptocurrencies such as Bitcoin, Z-coin and Monero continue play in darknet market operations and conclude by taking attendees on a real-time tour of several popular darknet markets.

Investigating the Millennial Mind: Understanding the Use and Impact of Technology on Today's Youth

In this session, we will have an update of the Adolescents and Technology session from two years ago discussing the investigative challenges of adolescents and millennials ESI. With help from the panel we will discuss the use of technology, communication platforms and types, looking at strategies for working with young people as suspects, witnesses, or victims. We'll also look at sources of evidence, cloud and app data, and discuss strategies for monitoring such as GPS location and cell tower records.

Modern Smartphones Investigation Issues, Solutions, and Methods

Smartphone are crucial to our lives and our businesses as well as the crimes involved in both. If you have not dealt with them yet, you will. Being prepared is key and learning the steps you need to walk through to produce the best possible results can save you hours of headache. This session will focus on a practical approach to the collection of data from smartphones as well as other associated devices and review of the methods that should be used with adding this capability to your team or check list for when these capabilities need to be outsourced.

Shh! Alexa is Listening: A Security Look at Voice-Based Assistants

Rapid developments in the field of artificial intelligence (AI) have resulted in a spate of new products and services. Without these advances, voice-based assistants like the Amazon Echo, Apple's Siri, Microsoft's Cortana, and others, could not exist. But just like too many other technologies of the past, voice-based assistants are being integrated into our daily lives without a complete understanding of the security risks they pose. In this session, attendees will be introduced to the security issues surrounding voice-based assistants. Attendees will be given a high-level overview of voice-based assistants and their evolving role as part of the Internet of Things (IoT). There will be a discussion of the listening capabilities of voice-based assistants, introduce attendees to several successful attacks on the Amazon Echo and close with a discussion of the potential and limitations of voice-based assistants as an investigative tool.

The Bits Behind the Coin: Uncovering the Cryptocurrency Trail During an Investigation

Bitcoin and other altcoins have been in the news almost daily lately. You may or may not be aware of what blockchain and/or cryptocurrencies are but news of the rapid increase of value, wild price fluctuations, major investment options, ransomware crypto payments and dark web activity it will be difficult to ignore cryptocurrencies and blockchain based transactions as relevant in digital investigations. During this session, we will familiarize you with the tools and processes to investigate and analyze blockchain and cryptocurrency activity.

The Use of Big Data to Enhance Enterprise Security

Buzzwords in security catch our eye as they begin to appear in articles, journals, and conferences. "Big Data" and "Security Analytics" are two such concepts. "User Entity Behavior Analytics" (UEBA) is another key term. Most organizations monitor security events produced from various systems. The problem is the collection, storage, security, and intelligent usage of these events has become unmanageable, meaning threats go undetected. An approach is to use a Big Data platform, such as Hadoop, to store the events. With this comes the advantage of security analytics with various Big Data tools. This session will explore the use of Big Data in security analytics and UEBA. We will also look at the supporting Hadoop ecosystem and its architecture and security.

Top 10 Cloud Security Threats and Solutions

Cloud computing has brought relief to enterprises by relieving them of managing huge IT infrastructure requirement and bringing down cost of IT related operations substantially. Cloud security is becoming important especially from the perspective of Data loss prevention, data security, privacy in lieu of multi-tenancy and how jurisdiction of the country influences the data in motion, data at rest, data in use. In this session, we'll identify the top 10 cloud security threats and provide practical solutions.

Vehicle Forensics: Obtaining Critical Data Through Infotainment and Telematics Vehicle Systems

Over the past several years, automotive manufactures have been adding advanced technology to seamlessly and safely integrate access to our digital lives from within our vehicles. Vehicles that create an experience that entertains and informs us as well as facilitates voice and data communications while we travel. With continued consumer demand of these sophisticated infotainment and telematics systems, the forensic benefit lies in the storage of vast amounts of data such as logging vehicle routes, odometer readings, call logs, contact lists, SMS messages, emails, pictures, videos, social media feeds, and in some cases velocity logs indicating hard braking and hard accelerations. All this data can be critical evidence in an active investigation. In this session, we'll discuss: What data can be acquired from infotainment and telematics systems within the vehicle; Non-destructive methods to acquire and analyze data; and share real life case studies at local and national levels.

When They Don't Want to be Found: A Look at Bitcoin and the Dark Web

Currency like Bitcoin, based on the cryptography principal, has added a layer of almost untraceable transactions to the already hard to navigate world of the Dark Web. Looking into a world where anything is up for sale, and trying to trace transactions and pull out viable, reliable evidence is difficult at best, impossible at worst. Join us to discuss the possible methods that can be used to recover and track evidence from the Dark Web and Bitcoin transactions. Learn more about where cryptocurrency is heading and what we investigators, examiners, and their teams need to be aware of.