Techno Security & Digital Forensics Conference

Myrtle Beach, SC | June 2-5, 2019 | Marriott Resort at Grande Dunes

2019 Event Guide

Blending together the digital forensics and cybersecurity industries for collaboration between government and private sectors.

www.TechnoSecurity.us

Host Sponsors: Cellebrite Digital intelligence for a safer world | MAGNET FORENSICS

COMEXPOSIUM
www.comexposium.com

MAGNET FORENSICS®

GRAYSHIFT

GET THE MOST DATA FROM iOS DEVICES.

Together, Magnet AXIOM and GrayKey let you acquire and analyze the most comprehensive data from unlocked and locked iOS devices.

magnetforensics.com/graykey

Techno Security & Digital Forensics Conference

Welcome to the 21st edition of the Myrtle Beach Techno Security & Digital Forensics Conference!

This brand has grown into one of the most important resources for corporate network security professionals, federal, state and local law enforcement digital forensic specialists, and cybersecurity industry leaders from around the world. The purpose is to raise international awareness of developments, teaching, training, responsibilities, and ethics in the field of IT security and digital forensics.

The 2019 program will feature 111 sessions led by 89 industry experts plus 56 exhibiting sponsors showcasing their latest tools, products and solutions.

We hope your time at the event proves to be rewarding and enjoyable. Please let our team know if there is anything we can do to make your participation more successful.

Your 2019 Event Management Team

Table of Contents

Schedule at a Glance 4
Networking Events 5
Keynote 6
Early Riser Session 6
Sunday Conference Program 8
Monday Conference Program 16
Tuesday Conference Program 28
Wednesday Conference Program 38
Exhibit Hall Floor Plan 44
Hotel Floor Plan 45
Sponsor Alphabetical Listing 46
Advisory Board 56
Industry Supporters 56

Stay Connected!

Download the **Techno Security Mobile App** in your App Store for full, up-to-date show details, speaker profiles, session presentations, and much more!

Search for:
Techno Security

Share photos of your experience with us using the **#TechnoSecurityMB** tag! Like us on Facebook and Follow us on Twitter and LinkedIn for updates and to stay connected with fellow attendees.

www.twitter.com/technosecurity

www.facebook.com/TechSecNA

Group:
Techno Security & Digital Forensics Conference

Sunday, June 2

12:00pm	–	12:50pm	Sessions
1:00pm	–	1:50pm	Sessions
2:00pm	–	2:50pm	Sessions
3:00pm	–	3:50pm	Sessions
3:00pm	–	7:00pm	Exhibit Hall Open
4:00pm	–	4:50pm	Sessions
5:00pm	–	6:30pm	Show Floor Happy Hour Reception

Monday, June 3

7:30am	–	8:00am	Continental Breakfast
8:00am	–	9:00am	Keynote
9:00am	–	9:30am	Networking Break
9:30am	–	10:20am	Sessions
10:30am	–	11:20am	Sessions
11:00am	–	4:30pm	Exhibit Hall Open
11:30am	–	1:30pm	Dedicated Exhibit Hall Hours
12:00pm	–	1:00pm	Lunch
1:30pm	–	2:20pm	Sessions
2:30pm	–	3:30pm	Networking Break in Exhibit Hall
3:30pm	–	4:20pm	Sessions
4:30pm	–	5:20pm	Sessions
5:30pm	–	6:30pm	Courtyard Reception (Sponsored by Oxygen Forensics in partnership with Project Vic & Whooster)

Tuesday, June 4

7:30am	–	8:00am	Continental Breakfast
8:00am	–	9:00am	Early Riser Session
9:00am	–	9:30am	Networking Break
9:30am	–	10:20am	Sessions
10:30am	–	11:20am	Sessions
11:00am	–	3:30pm	Exhibit Hall Open
11:30am	–	1:30pm	Dedicated Exhibit Hall Hours
12:00pm	–	1:00pm	Lunch
1:30pm	–	2:20pm	Sessions
2:30pm	–	3:30pm	Networking Break in Exhibit Hall
3:30pm	–	4:20pm	Sessions
4:30pm	–	5:20pm	Sessions
5:30pm	–	6:30pm	Courtyard Reception

Wednesday, June 5

8:30am	–	9:00am	Continental Breakfast
9:00am	–	9:50am	Sessions
10:00am	–	10:50am	Sessions
11:00am	–	11:50am	Sessions

On top of the informative conference program and exhibit hall, event management continues to strive to provide attendees and sponsors with ample time to network and develop relationships both on and off the show floor.

In addition to the lunches, breakfasts, and breaks, the 2019 event will feature evening receptions all three nights.

Sunday, June 2

Show Floor Happy Hour Reception | 5:00pm – 6:30pm

Join the industry for the event kickoff reception on the show floor for drinks, networking, and a first look at what the 2019 sponsors are featuring in the exhibit hall.

Monday, June 3

Oceanfront Courtyard Reception | 5:30pm – 6:30pm

Unwind outside overlooking the ocean after a full event day. The reception will take place on the oceanfront courtyard with food, drinks, and networking.

Sponsored by: OXYGEN FORENSICS, WHOOSTER, PROJECT VIC

Tuesday, June 4

Oceanfront Courtyard Reception | 5:30pm – 6:30pm

Join the industry for an outdoor reception to enjoy the last evening of the event with appetizers, drinks, and good company.

Sherri Davidoff

CEO, LMG Security and BrightWise, Inc.

Emerging Threats and How to Counter Them

Monday, June 3 | 8:00am – 9:00am

Sherri Davidoff is a cybersecurity expert, author, speaker and CEO of both LMG Security and BrightWise, Inc. She has conducted cybersecurity training for many notable organizations, including the Department of Defense, the American Bar Association, FFIEC/FDIC, and many more. Sherri is a faculty member at the Pacific Coast Banking School, where she teaches cybersecurity classes. She is a frequent contributor of education articles and webinars, and occasionally serves as a cybersecurity expert on television. Sherri is a GIAC-certified forensic examiner (GCFA) and penetration tester (GPEN), and holds her degree in Computer Science and Electrical Engineering from MIT. Her new book, *"Data Breaches,"* will be released in the spring of 2019.

Refer to page 16 for full session details

Early Riser Session

Dark Web, Version 2: The New Challenge for LE

Tuesday, June 4 | 8:00am – 9:00am

Presented by: Stephen Arnold, Commissioner, International Tribunal for Justice

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.

Refer to page 28 for full session details

Catch **OXYGEN FORENSICS** on stage at
Techno Security & Digital Forensics Conference

MONDAY, JUNE 3

OXYGEN FORENSIC® JETENGINE

RESULTS IN RECORD TIME

9:30 a.m. - 10:20 a.m.

MONDAY, JUNE 3

INTERNET OF EVERYTHING

4:30 p.m. - 5:20 p.m.

TUESDAY, JUNE 4

REVOLUTIONIZING DFIR:

INNOVATIONS, ADVANCEMENTS, AND GAME-CHANGING TECHNOLOGY FOR INVESTIGATORS

10:30 p.m. - 11:20 p.m.

Booth 403

Sunday, June 2

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management **Forensics** **Information Security** **Investigations** **Cellebrite Lab** **Magnet Forensics Lab** **Sponsor Demo**

12:00pm – 12:50pm

Oleander A

Encryption for Everyday Applications

Nima Zahadat, Professor of Digital Forensics and Data Science, TASC

This session will cover encryption uses for day-to-day uses including application to email, browsing, mobile applications, and desktop applications. Several tools and techniques of encryption for day-to-day use will be demonstrated. Advanced applications of encryption like hiding of an OS and hiding of entire files will also be covered.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Investigators

Oleander B

Case Study: Digital Evidence in Fraud Investigations

Ed Michael, Detective, Orlando Police Department
Richard Colangelo, State's Attorney, Judicial District of Stamford/Norwalk

Take your fraud cases beyond bank records, photocopies, and manual searching. In this review of two major fraud cases, learn how to leverage all aspects of digital evidence from mobile, to computers, to cloud based data. This session will walk you through each step of the investigation, from the initial contact to how to present the massive amounts of evidence to the prosecutor and in court. You will walk away with the knowledge to work these cases quickly and completely, along with sample court orders to use for the various aspects of your cases.

Target Level: All Levels
Target Audience: Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Tides 1/2

Common Repairable iPhone Logic Board Problems: Fix the Board, Recover the Data

Jessa Jones, Owner, iPad Rehab Microsoldering

For encrypted data on iOS and other mobile devices, the path to data recovery often requires getting the device to turn on and boot natively. This can be a hardship for many devices that have accidental or intentional damage to the logic board hardware. Fortunately, many of these faults are repairable with low cost microsoldering equipment and some training. This session will showcase some of the common "signature faults" that occur in iPhones, and show you what the repair of these faults looks like. This session will cover short circuit detection and repair, charger damage, and common micro-bga chip problems from flexion-damage that occurs every day in larger form iPhones. 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. During the session, the presenter will walk you through a live example of a dead iPhone with a logic board hardware problem, and invite audience volunteers to use our handheld thermal camera to find the cause of a short circuit, and to bring the phone back to life in real time!

Target Level: Beginner
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Atlantic 3

Advanced DVR Analysis Case Studies

Jimmy Schroering, CTO, DME Forensics

This session will discuss several cases where the scope of the examination exceeded a simple DVR recovery. These types of advanced examinations require a significant understanding of the operation of the DVR system in question in order to render opinions and conclusions based on the analysis. While more time consuming than a simple recovery, these cases demonstrate the potential for providing more value to the investigation.

Target Level: Intermediate
Target Audience: Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

12:00pm – 12:50pm (continued)

Atlantic 2

Supporting the Unsupported: Carving, Parsing, and Creating Custom Artifacts:
Christopher Vance, Manager, Curriculum Development, Magnet Forensics

Hands-On Lab: Many of the new mobile applications that daily hit the App Store and Google Play contain features that can contain crucial evidence. Often, though, commercial forensic tools cannot keep pace with these apps or their consumer usage. This lab will describe how to acquire evidence from a wide range of smartphones including Samsung, LG, Qualcomm, and off-brand devices using MTK chips. The presenter will review methods to discover and parse data from unsupported applications, including the chat, contact, location, and historical data that can be found using AXIOM's Dynamic App Finder. Finally, the presenter will discuss how to create custom artifacts to parse and carve data from the unsupported databases.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Law Enforcement/Police

Atlantic 1

Maximize Your Data Access Utilizing New Physical Analyzer Capabilities
Danny Garcia, Senior Director of Certification and Learning Technology, Global Training Division, Cellebrite

Hands On Lab: This demo will cover the various methods you can apply to acquire maximum data from the growing number of Apple and Android applications including those unsupported through traditional decoding methods. Learn how to use the SQLite Wizard to recover data within unparsed SQLite databases, understand how to search and highlight unparsed data and how to apply image carving and location carving to expose hidden artifacts. Perform this while recording your every step to maintain the integrity of the data. Finally, the speaker will demonstrate our latest innovation for extracting locations, contacts, user accounts and more from any database on the device with the Cellebrite App Genie.

Target Level: Intermediate
Target Audience: Government, Law Enforcement/Police, Corporate/Private Sector

Sunday, June 2 (continued)

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management **Forensics** **Information Security** **Investigations** **Cellebrite Lab** **Magnet Forensics Lab** **Sponsor Demo**

1:00pm – 1:50pm

Oleander A

More Substance Than Vapor: When and Why to Include Evidence from the Cloud in Your Investigations
Trey Amick, Forensics Consultant, Magnet Forensics

In a landscape of digital change, cloud storage has come to be a constant. Spanning mobile devices, computers, the Internet of Things (IoT), and more, cloud storage is an important data source—and sometimes, the only accessible source—for investigators in both public and private sectors. Even so, legal or procedural concerns, or simply a focus on device storage, prevent many investigators from obtaining this data. In this session, prepare to delve into the differences between cloud storage and device storage, including what's available on each type of device. Find out why and how you may be missing important data, and get a sense for the scope of this missed potential. Finally, understand what's possible from a procedural standpoint so that you can turn obstacles into opportunities.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Law Enforcement/Police

Oleander B

Blockchain and eDiscovery: The Legal Impact of BlockChain Technology
John Wilson, President, HaystackID, LLC

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 them understand how to examine and investigate these technologies and the electronically stored information that results from their usage.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Tides 1/2

Making Complex Issues Simple: A Unique Method to Extract Data from RAID with Lost Configuration
Mike Vysochin, Senior Data Recovery Engineer/Training Instructor, ACE Lab

Previously, only large enterprises have chosen RAID as storage media, now they are also commonly found among small companies and domestic users (e.g. home NAS). Therefore, it increases the possibility that RAID can be used in criminal activities and encountered by a digital forensics examiner. To gain access to data on RAID, it's necessary not only to create a forensic image of each drive but also to assemble the array. But what if the service structures with the description of the configuration are damaged or lost? In such a case, the expert has to determine the correct configuration of a RAID out of thousands, or even millions of possible variants. During the session, attendees will discover technologies and practical methods which will make this hard work considerably easier and faster.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Atlantic 3

Deriving Intelligence Requirements from Risk Management Artifacts
Kristi Horton, Founder, Horton Innovations, LLC

Law enforcement, government agencies, and private sector critical infrastructure organizations have been encouraged to develop cyber intelligence capabilities as part of a well rounded information security program. The field of intelligence has existed for millennia. We do not have to re-invent intelligence practices to apply them to the cyber domain. We do need to learn and remember the lessons from our past successes and failures. In this session, the presenter will relay one helpful tactic she used in beginning an intelligence function in the private sector and explain how to derive and propose intelligence requirements to decision makers who will use analytic results in their every day lives.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators

1:00pm – 1:50pm (continued)

Atlantic 2

Using GrayKey and AXIOM to Acquire and Parse iOS Data that Other Tools Miss

Christopher Vance, Manager, Curriculum Development, Magnet Forensics
David Miles, Co-Founder, Grayshift

Hands-On Lab: Learn about the game-changing GrayKey device and its ability to go beyond backup files to get at file system, process memory, and keychain data. Find out how these capabilities extend across the versions and sub-versions of iOS 10, 11, and 12, and learn how to use a GrayKey device to extract data. Additionally, learn how to use Magnet AXIOM to ingest and process the data, put it together with other data such as what's available from iCloud, and extend your findings with exclusive-to-AXIOM capabilities such as the Dynamic App Finder, SQLite viewers, and Plist viewers.

Target Level: Intermediate
Target Audience: Government, Law Enforcement/Police

Atlantic 1

Fourth Amendment Search and Seizure of Digital Data

Judge Mark McGinnis, Judge, State of Wisconsin

This session will discuss the fundamental framework of the 4th Amendment and provide information regarding the legal framework of searching and/or seizing digital data. There will be a focus on what constitutes a "search" of digital data, what constitutes a "seizure" of digital data, when there is a reasonable expectation of privacy in digital data, when a warrant is required, the exceptions to the search warrant requirement and their applicability to digital data, the drafting and execution of search warrants for digital data, and the current hot topics in this area.

Target Level: All Levels
Target Audience: Government, Law Enforcement/Police

Sunday, June 2 (continued)

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management | Forensics | Information Security | Investigations | Cellebrite Lab | Magnet Forensics Lab | Sponsor Demo

2:00pm – 2:50pm

Oleander A

OSINT Forensics: How to Determine if Your Subject Has Been Visiting the Deep or Dark Web?
Anthony Reyes, International President, HTCIA

During this session attendees will learn what type of software's are used to access the Dark and Deep webs. They will learn what types of forensic artifacts can be found from these software's. The presenter will try to determine the locations visited by the user. In addition, the presenters will examine how to build a case to prove that your subject has been engaged in illegal activities on the Dark or Deep webs in a manner that will hold up in court.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Tides 1/2

A.I. See You: Leveraging Deep Learning to Triage Pictures and Video
Matt McFadden, Director of Training, BlackBag Technologies

There can be hundreds of thousands of images on digital devices. Where does an examiner start? Techniques based on file size, date created, and hash sets are a good start, but are insufficient for the sheer volume of data examiners must sort through. What if investigators could view files with specific types of images first? Learning engines can be trained to identify pictures or videos that likely depict categories like weapons, pornography, drugs, and graphic violence. When combining image categorization with previous prioritization techniques, investigators can more quickly triage a device allowing them to look at the best candidates that may be relevant to their case. Learn how these models are trained, how to appropriately use them, and why it is essential to understand their power and limitations. From assessing which devices need to be seized onsite, to reviewing employee's adherence to an acceptable use policy, these techniques save time by highlighting for examiners pictures and videos with questionable content.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Atlantic 3

Fostering a Resilient Cybersecurity Culture: The Keys to Success in Creating a Talented and Engaged Cyber Workforce
Matt Donato, Co-Founder & Managing Partner, HuntSource

By now, everyone is aware of the challenges we face combatting the imminent adversarial cyber threats. The solution, however, is complex and continues to be debated. In particular, the emphasis on closing the gap in the cybersecurity workforce has become the leading contender of what is most urgent and important in our industry. Organizations that make investments in cybersecurity technology have also come to the realization that they, too, need to acquire and retain the requisite subject matter expertise to strengthen their organizational posture. During this session, the presenter will share the keys to success in creating a talented, satisfied, and engaged cybersecurity workforce. In addition, the presenter will discuss the various best practices firms can use to identify, attract, and develop talent to fit their organizational challenges.

Target Level: All Levels
Target Audience: Corporate/Private Sector

Atlantic 2

Forensics in the Corporate Cloud: How to Conduct Office 365 and Google Suite Investigations
Jamey Tubbs, Director, Training Operations, Magnet Forensics

Hands-On Lab: As enterprises of all sizes continue to shift data into cloud-based content storage and collaboration platforms, the evidence of all kinds of threats both internal and external lives less on hard drives or smartphones, and more on cloud servers. In this lab, learn how to use AXIOM Cloud to recover forensically sound content, metadata, and audit logs using administrative credentials from Microsoft (R) Office (R) 365 and Google Suite services. In addition, learn how to use Connections in AXIOM to tie cloud artifacts to computers and smartphones to see the full picture, demonstrate intent, and construct robust timelines for a complete story.

Target Level: Intermediate
Target Audience: Corporate/Private Sector

2:00pm – 2:50pm (continued)

Atlantic 1

The Art of the Possible: End-to-End Best Practices to Close Your Most Challenging Investigations

Richard Colangelo, State's Attorney, Judicial District of Stamford / Norwalk
Ed Michael, Detective, Orlando Police Department

In 2017 the Norwalk Police Department was called to investigate the suspicious death of Kadeelyn Konstantino. As the investigation unfolded, investigators and prosecutors were able to locate evidence that implicated Lori Ledonne as the person who unlawfully supplied Konstantino with a lethal cocktail of heroin and fentanyl. She was subsequently charged, convicted and sentenced to prison for the unlawful sale of narcotics and the death of Kadeelyn Konstantino. Fast forward to 2018, Connecticut State's Attorney Rich Colangelo will now leverage the power of Cellebrite's Digital Intelligence solutions to re-examine the digital evidence as a case study in how to optimize investigations using the latest forensics tools. During this session, Colangelo will utilize Cellebrite's UFED, Physical Analyzer, Public Cloud and Analytics Enterprise solutions, to extract digital evidence and show how these tools can support complex investigations.

Target Level: All Levels
Target Audience: Government, Law Enforcement/Police, Corporate/Private Sector

2:00pm – 3:50pm

Oleander B

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

Moderator: Derek Ellington, Certified Digital Forensic Examiner, Ellington Digital Forensics
Panelists: Roxanne Ellington, Certified Substance Abuse Counselor, Youth Addictions Specialist, Duke University (Ret.)
Jessica Coates, Certified Digital Forensic Examiner, Ellington Digital Forensics
Ben Levitan, Telecommunications and Cellular Expert, Ben Levitan LLC

This session will present an update of the Adolescents and Technology session from two years ago discussing the investigative challenges of adolescents and millennial's ESI. The panel will discuss the use of technology, communication platforms and types, looking at strategies for working with young people as suspects, witnesses, or victims. The panel will also look at sources of evidence, cloud and app data, and discuss strategies for monitoring such as GPS location and cell tower records.

Target Level: Beginner
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

3:00pm – 3:50pm

Oleander A

High Profile Investigations and How Technology Today Impacts Them

Chris McDonough, Senior Vice President, Business Development, Whooster
Richard Spradley, CEO, Whooster

As an investigator, you never know when a high-profile investigation suddenly arises in your area. Time is always of the essence and public demand for a quick resolution can add a tremendous amount of pressure towards the investigative team. While techniques have remained constant over the years, technology to leverage the answer you're seeking have changed dramatically and continue to ever evolve today. During this session, attendees will learn how to leverage various open source technologies available today (and what's on the horizon) to find the most efficient ways to gain answers when those situations arise in your area.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Tides 1/2

Hack Yourself, Before the Hackers Do

Steve McGregory, Sr Director, Application and Threat Intelligence, Ixia a Keysight Business

You've probably heard the phrase, "knowledge is power", and you understand what it means, but have you applied this to your current state of your cybersecurity defenses? This session is all about how knowledge of your cybersecurity people, processes and tools will make you more powerful. If you don't know how these will respond when under a cyber attack, then you will be left powerless to properly handle the situation. During this session, attendees will learn about techniques and tools anyone can deploy to help you assess your people, processes and tools.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police

Sunday, June 2 (continued)

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management · Forensics · Information Security · Investigations · Cellebrite Lab · Magnet Forensics Lab · Sponsor Demo

3:00pm – 3:50pm (continued)

Atlantic 3

Forensic Acquisition of Modern Evidence: A Roadmap to What's Changed

Bradley Schatz, Director, Evimetry

Forensic acquisition isn't the known quantity that it was. With new storage devices like SSD's and NVMe, new filesystems like APFS, and computers increasingly become locked down, the old techniques and assumptions will only get you so far. This session will examine where the old techniques fail or are a poor choice for today's evidence sources; teach forensically sound techniques for acquiring modern computer, mobile, and cloud evidence; and identify new techniques for accelerating forensic workflow.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police

Atlantic 2

From Dead Box to Live Memory: Breathing Context into Forensic Investigations

Jamey Tubbs, Director, Training Operations, Magnet Forensics

Hands-On Lab: Traditionally the domain of experienced forensic examiners, memory analysis can provide access to evidence you can't obtain through "dead-box" forensics alone. In many cases, memory analysis may be the only way to obtain evidence critical to solving your investigation. Using cybercrime and cybersecurity incident response case studies, this lab will discuss how AXIOM's integration of core plugins from the popular tool, Volatility, makes deep memory analysis more accessible to forensic examiners. In addition, learn how to incorporate memory artifacts into a broader timeline together with artifacts from other data sources for a well-rounded investigation.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Law Enforcement/Police

Atlantic 1

Cloud Forensics for Your Investigation

Justin Cole, Manager of Contractors for Special Projects, Cellebrite
John McHenry, Director Curriculum, Cellebrite

Learn about Cellebrite's UFED Cloud Analyzer and how you can use it to recover forensically sound content, from more than 40 cloud applications and sources. This session will describe how to export an account package and how to ingest it into UFED Cloud Analyzer. The presenters will show how to use the password collector to retrieve credentials saved on mobile browsers and apply them in the product to retrieve cloud data. In addition, the presenters will review features like Web Capture, getting public data in UFED Physical Analyzer and how to apply an iCloud Backup when an actual device is not available. The session will also walk through best practices for acquiring cloud warrants.

Target Level: All Levels
Target Audience: Government, Law Enforcement/Police, Corporate/Private Sector

4:00pm – 4:50pm

Oleander A

Detecting and Investigating Malicious PowerShell

Hoke Smith, Director, Cybersecurity and Analytics, Nuix USG

PowerShell is a favorite tool of a range of threat actors. State actors, criminal gangs, and individual hackers have all incorporated PowerShell in highly effective "fileless" attacks, resulting in damaging compromises. While PowerShell usage can be detected in real time, distinguishing legitimate from malicious use can be challenging. In this session, attendees will learn: How PowerShell is typically used in fileless attacks; How malicious use can be distinguished from legitimate use; Useful techniques to investigate PowerShell in both real time (live streamed); and Post-event (forensics) datasets.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators

4:00pm – 4:50pm (continued)

Oleander B

New USB Forensics

Bob Osgood, SSA - FBI Retired/Director - Digital Forensics & Cyber Analysis, George Mason University

USB forensic artifacts have been used by examiners for years; however, earlier this year, it was revealed with Windows 10 that a new event log, the Microsoft-Windows-Partition%4Diagnostics.evtx (MWPD) file emerged with event ID 1006 containing detailed information of removable devices. During this session, attendees will be provided a detailed introduction to MWPD, learn how these artifacts differ from previous forensics artifacts, and how to effectively mine this potential wealth of forensic information.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Tides 1/2

Telegram Messenger Investigation on Mobile Devices

Yuri Gubanov, CEO and Founder, Belkasoft USA

With 200M+ audience worldwide, Telegram Messenger is one of the most popular chat apps. Due to its increasing popularity it is met more and more often in digital investigations. This session will cover various artifacts left after Telegram for iOS and Android devices. The presenter will go through the most important structures used to store data and will even recover some deleted secret chats!

Target Level: Advanced
Target Audience: Investigators, Law Enforcement/Police

Atlantic 3

Data Recovery From Damaged MicroSD Cards and Other Monolithic Devices

Igor Loskutov, Engineer, Rusolut

MicroSD cards became a true standard for portable storage devices. Due to high capacity and tiny size they are used now even for less conventional applications such as drones, video monitoring systems and so on. When forensic laboratories receive damaged memory cards for analysis it is not an easy job to extract data out of it, considering that NAND memory and controller are embedded together into solid package. The case gets even worse if device is physically damaged. In this session, the presenter will go through the whole process of data reconstruction and challenges that experts face.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Atlantic 2

Cloud Forensics for Law Enforcement: Get the Evidence You Need to Move Cases Forward

Jamey Tubbs, Director, Training Operations, Magnet Forensics

Hands-On Lab: Evidence stored in servers belonging to service providers like Facebook and Google can be crucial in a law enforcement investigation and also among the hardest to acquire. Even when you can get a warrant to force a provider to return data, collecting the data into a normalized, easy-to-analyze format can be tricky. This lab will focus on Facebook's warrant return support and Download Your Information features for both Facebook and Instagram. The presenter will describe how to ingest data into AXIOM Cloud and use commercial innovations to save time during investigations. The presenter will also discuss how to acquire photos from Twitter without requiring user credentials, and features such as Magnet.AI that can help you identify key pieces of evidence.

Target Level: Intermediate
Target Audience: Government, Law Enforcement/Police

Atlantic 1

The Admissibility of Digital Data

Judge Mark McGinnis, Judge, State of Wisconsin
Ed Michael, Detective, Orlando Police Department

This session will discuss admissibility issues involving digital data including authenticity, foundation, relevance, hearsay, the confrontation clause, and when expert testimony is required. The presenters will provide a legal framework that analyzes the admissibility of digital data into evidence.

Target Level: All Levels
Target Audience: Government, Law Enforcement/Police, Corporate/Private Sector

Monday, June 3

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management **Forensics** **Information Security** **Investigations** **Cellebrite Lab** **Magnet Forensics Lab** **Sponsor Demo**

8:00am – 9:00am

Oleander A/B **Keynote: Emerging Threats and How to Counter Them**
Sherri Davidoff, CEO, LMG Security

Cybercriminals are taking hacking to the next level, by leveraging ever-more-sophisticated tool-sets and increasingly mature techniques. Ransomware, banking trojans, and cryptojacking are constantly evolving new features, designed to maximize the payout for criminals. This fast-paced keynote will explore these new attack techniques and other high-risk developments, using screenshots and videos from real cases. Learn about these top threats and solutions to combat them in order to protect your organization and community today, and in the future.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigations, Law Enforcement/Police, Prosecutors/Attorneys/Legal

9:30am – 10:20am

Oleander A **UAS Forensics - Visualizing the Data**
Greg Dominguez, Founder/CEO, GCD Forensic Consulting, LLC
David Kovar, Founder/CEO, URSA, Inc.

This 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 presenters will guide you through the process of selecting and visualizing the data to answer specific questions in a vendor agnostic approach.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Oleander B **Opioid Crisis in America: From Digital Clues to a Murder Conviction**
Ed Michael, Detective, Orlando Police Department

Every day, more than 115 people in the United States die after overdosing on opioids. The misuse of and addiction to opioids including prescription pain relievers, heroin, and synthetic opioids such as fentanyl is a serious national crisis that affects public health as well as social and economic welfare. Every life style and walk of life has seen the destruction and death opioids and fentanyl can do to families. Using extraction and analytics tools, learn how to successfully gather intelligence from scenes and witnesses to prosecute the dealers and suppliers. Given by Detective Ed Michael of the Orlando Police Department, this lab was pivotal in getting one of the first murder convictions in Florida for an opioid death using mainly digital evidence.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Tides 1/2 **Introduction to Security Architecture for Big Data: How to Securely Use Your Big Data Ecosystem**
Mark Graves, Head, Enterprise Security Architecture, TD Bank Group

More and more enterprises are using Big Data for business applications and analytics. Security analytics applications also use Big Data. Placing so much data in on a shared ecosystem certainly has its advantages, but risk must also be managed. Along with the advantages, there are some unique challenges to using a Big Data ecosystem securely. This session will examine Big Data security architecture to help you securely implement Big Data in your organization. Taking a security architecture approach allows attendees to consider security capabilities regardless of specific platforms. The presenter will also consider specific use cases and how the big data security architecture supports them.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government

9:30am – 10:20am (continued)

Atlantic 2

Forensics in the Corporate Cloud: How to Conduct Office 365 and Google Suite Investigations
Jamey Tubbs, Director, Training Operations, Magnet Forensics

Hands-On Lab: As enterprises of all sizes continue to shift data into cloud-based content storage and collaboration platforms, the evidence of all kinds of threats both internal and external lives less on hard drives or smartphones, and more on cloud servers. In this lab, learn how to use AXIOM Cloud to recover forensically sound content, metadata, and audit logs using administrative credentials from Microsoft(R) Office(R) 365 and Google Suite services. In addition, learn how to use Connections in AXIOM to tie cloud artifacts to computers and smartphones to see the full picture, demonstrate intent, and construct robust timelines for a complete story.

Target Level: Intermediate
Target Audience: Corporate/Private Sector

Atlantic 1

Get the Data You Need in Less Than 20 Minutes with Selective Extraction
Danny Garcia, Senior Director of Certification and Learning Technology, Global Training Division, Cellebrite
Justin Cole, Manager of Contractors for Special Projects, Cellebrite

When time is of the essence and you are tasked with reviewing evidence that you suspect resides on a specific app or in a cloud source, learn how to perform a full-file system selective extraction. Understand how you can determine if a device is worth investigating based on the profile and properties, see how you can pick and choose the application you want to review. Decode the data and present it in its native form with the Virtual Analyzer app simulator. The presenters will demonstrate how you can use the cloud tokens retrieved to access SnapChat data including SnapChat MyEyes only.

Target Level: All Levels
Target Audience: Government, Law Enforcement/Police, Corporate/Private Sector

Monday, June 3 (continued)

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management **Forensics** **Information Security** **Investigations** **Cellebrite Lab** **Magnet Forensics Lab** **Sponsor Demo**

9:30am – 10:20am (continued)

Heron

Oxygen Forensic JetEngine – Results in Record Time
Lee Reiber, COO, Oxygen Forensics

This workshop session will explain how attendees can use Oxygen Forensics' free and innovative 64-bit JetEngine utility to quickly parse large volumes of data and leverage advanced analytical tools to quickly pinpoint evidence in record time. In digital forensics investigations, the most important aspects are time and efficiency. Oxygen Forensic® JetEngine delivers parsing and decoding of the data 3 times faster to support massive and varied data sets from mobile devices, their backups and images, drone flight logs and cloud services. Attendees will learn a new multi-tab user interface, use advanced cross-device sections and tag manager, and find relevant evidence across multiple devices and accounts with elegance and ease. Attendees will also learn to use Oxygen Forensic® JetEngine together with the main Oxygen Forensic® Detective software to cut the time spent retrieving and sifting through data and do what matters most: delivering results.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police

Osprey

Virtual Pen Registers™
Sy Ray, President, ZetX

An introduction to a CJIS compliant cloud based Pen Register solution for law enforcement.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

9:30am – 11:20am

Atlantic 3

The Questions a Judge Will Ask You After a Data Breach
Tod Ferran, Managing Consultant, HALOCK Security Labs

During this session, attendees will understand: How to define "reasonable" in a way that makes sense to business, judges, and regulators; How to design and run a risk assessment that is meaningful to technicians, business, and authorities; and Learn from case studies involving regulatory oversight, law suits that happened, and law suits that never happened.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Prosecutors/Attorneys/Legal

10:30am – 11:20am

Oleander A

Chrome Nuts and Bolts: ChromeOS/Chromebook Forensics
Jessica Hyde, Director of Forensics, Magnet Forensics

Chromebooks have been taking over the classroom and are an up and coming issue for forensic examiners. This session will delve into our research into the forensics of the Chrome OS and Chromebooks. The presenter will dive into the hardware and software perspectives of how to deal with a Chromebook in an investigation and provide practical techniques to help you with your analysis.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Law Enforcement/Police

10:30am – 11:20am (continued)

Oleander B

Hackers, Hooligans, Heists, & History

Christine Stevenson, Security Engineer, Verodin

This session will explore an abridged history of hackers, hooligans, and heists. It will also examine new ways of approaching cybersecurity to mitigate nefarious acts by focusing on actual security effectiveness instead of the latest APT, 0-day, and regulatory mandate. The presenter will translate the "who, how, and why" of cyberattacks. The presenter will also identify multiple "old school" and modern-day threat vectors and organize attacks by motives like sabotage and espionage. Each threat actor type will be explored in detail with real-life use cases and personal accountants. The examples used will illustrate the diversity in threats, methods, motivations, and organizational responses.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Tides 1/2

Cellular Technology, Mapping, & Analysis

Scott Eicher, Director of Professional Services, Hawk Analytics, Inc.

This session will provide an in-depth look into cellular networks and call detail records (CDR's) from any cell phone provider. The presenters will share how to understand CDRs, how to use CDRs and why it is critical to investigations. Attendees will also learn the common problems with CDRs that must be addressed to be able to map them correctly while also going through a real-life case study where CDRs were crucial in the arrest and conviction of violent felons.

Target Level: Beginner
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Monday, June 3 (continued)

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management **Forensics** **Information Security** **Investigations** **Cellebrite Lab** **Magnet Forensics Lab** **Sponsor Demo**

10:30am – 11:20am (continued)

Atlantic 2

From Dead Box to Live Memory: Breathing Context into Forensic Investigations

Jamey Tubbs, Director, Training Operations, Magnet Forensics

Hands-On Lab: Traditionally the domain of experienced forensic examiners, memory analysis can provide access to evidence you can't obtain through "dead-box" forensics alone. In many cases, memory analysis may be the only way to obtain evidence critical to solving your investigation. Using cybercrime and cybersecurity incident response case studies, this lab will discuss how AXIOM's integration of core plugins from the popular tool, Volatility, makes deep memory analysis more accessible to forensic examiners. In addition, learn how to incorporate memory artifacts into a broader timeline together with artifacts from other data sources for a well-rounded investigation.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Law Enforcement/Police

Atlantic 1

The Art of the Possible: End-to-End Best Practices to Close Your Most Challenging Investigations

Richard Colangelo, State's Attorney, Judicial District of Stamford/Norwalk
Ed Michael, Detective, Orlando Police Department

In 2017 the Norwalk Police Department was called to investigate the suspicious death of Kadeelyn Konstantino. As the investigation unfolded, investigators and prosecutors were able to locate evidence that implicated Lori Ledonne as the person who unlawfully supplied Konstantino with a lethal cocktail of heroin and fentanyl. She was subsequently charged, convicted and sentenced to prison for the unlawful sale of narcotics and the death of Kadeelyn Konstantino. Fast forward to 2018, Connecticut State's Attorney Rich Colangelo will now leverage the power of Cellebrite's Digital Intelligence solutions to re-examine the digital evidence as a case study in how to optimize investigations using the latest forensics tools. During this session, Colangelo will utilize Cellebrite's UFED, Physical Analyzer, Public Cloud and Analytics Enterprise solutions, to extract digital evidence and show how these tools can support complex investigations.

Target Level: All Levels
Target Audience: Government, Law Enforcement/Police, Corporate/Private Sector

Heron

SQLite forensics and Memory Forensics with Belkasoft Evidence Center, All-in-One Forensic Solution

Yuri Gubanov, CEO and Founder, Belkasoft USA

With the latest versions of Belkasoft Evidence Center (BEC), you can analyze mobile and computer devices, volatile memory, download and investigate cloud data, conduct remote forensics and incident response. During this demo, you will get a solid overview of the product features; we will discuss new trends and recently introduced artifacts, supported by BEC. In particular, we will cover restoring deleted data from SQLite, including Telegram secret chats, and memory analysis, including carving SQLites from RAM dumps.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Investigators, Law Enforcement/Police

Osprey

The Next Generation of AI Technology Comes to Law Enforcement

Jim Plitt, CEO, T3K/US, a subsidiary of T3K- Forensics, GmbH

T3K, Law Enforcement's Global Partner presenting its AI solutions including: LEAP: Law Enforcement Analytic Product (triaging and analytical tool applicable for border control, anti-terrorism and anti-trafficking) and PredatorNet: most powerful visual AI architecture employed in detecting Child Sexual Abuse Imagery.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

1:30pm – 2:20pm

Oleander A

Social Media Analysis and Counter-Terrorism
Abdul Hassan, CEO, INTCTFF

This session will delve into locating and extracting social media artifacts on mobile phones using available forensics tools, conducive to an investigation. Taking this knowledge, the session will then cover how using these artifacts are invaluable in both preventing and solving terror attacks. The Orlando Pulse Nightclub and San Bernardino attacks will be presented as case studies to provide specific examples of where social media has played a major part in indoctrinating extremist ideology.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Oleander B

Protecting Your Identity When Performing Online Investigations
Zuly Gonzalez, Co-Founder & CEO, Light Point Security

The web is a powerful tool for criminal investigators who use it to gather information about criminals, and learn about their activities, interests and motivations. However, online investigators need to take extra precautions to hide their identities, and protect themselves and their organizations from the criminals they are targeting. Many of the tools used today by investigators to anonymize their online identities can inadvertently reveal information about them, and tip their hands during a critical investigation. In this session, attendees will learn about the various tools you can use to browse the web anonymously, how to use them properly, and the pitfalls of each.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Monday, June 3 (continued)

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management | Forensics | Information Security | Investigations | Cellebrite Lab | Magnet Forensics Lab | Sponsor Demo

1:30pm – 2:20pm (continued)

Tides 1/2

Bringing Data Analytics Into Your Investigation

Steven Konecny, Director, EisnerAmper

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.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Atlantic 3

Forensic Certifications: Why, Which, and in What Order

Jared Coseglia, Founder/CEO, TRU Staffing Partners
Nathan Mousselli, Marine, Secret Service, Dept of Homeland Security
Doug Brush, Vice President, Cyber Security Solutions

The evolution of the digital forensic and investigations job market over the next decade will usher in a new and hyper-focused valuation of functional domain and software certification. DFIR professionals who may or may not have formalized their hands-on experience are now competing against a growing population of forensic savvy professionals, many with advanced degrees, looking for vertical mobility. Additionally, untraditional professionals, including lawyers, from tertiary disciplines are looking to break into areas of advisory and delivery employment surrounding breach prevention planning, remediation, and risk consultation. During this panel discussion, you'll get a better understanding of the DFIR certification ecosystem for non-software and tool specific accreditation. We will also cover opensource technology every DFIR pro should have in their toolkit. Panelists will discuss their certifications—which overlap many functional domain certifications with elements of project management, information governance, security, discovery, blockchain and analytics—and also provide potential career mapping pathways to help you expand and diversify your areas of expertise.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Atlantic 2

Using GrayKey and AXIOM to Acquire and Parse iOS Data that Other Tools Miss

Christopher Vance, Manager, Curriculum Development, Magnet Forensics
David Miles, Co-Founder, Grayshift

Hands-On Lab: Learn about the game-changing GrayKey device and its ability to go beyond backup files to get at file system, process memory, and keychain data. Find out how these capabilities extend across the versions and sub-versions of iOS 10, 11, and 12, and learn how to use a GrayKey device to extract data. Additionally, learn how to use Magnet AXIOM to ingest and process the data, put it together with other data such as what's available from iCloud, and extend your findings with exclusive-to-AXIOM capabilities such as the Dynamic App Finder, SQLite viewers, and Plist viewers.

Target Level: Intermediate
Target Audience: Government, Law Enforcement/Police

1:30pm – 2:20pm (continued)

Atlantic 1

Accelerating Your Investigation with Video Evidence & Analytics
Moderator: Buddy Tidwell, Vice President of Global Training, Cellebrite
Panelist: Jimmy Schroering, CTO, DME Forensics
Andrew Fredericks, Project Manager, iNPUT-ACE
Justin Cole, Manager of Contractors for Special Projects, Cellebrite

Please join us for an open panel discussion with DME Forensics, iNPUT-ACE and Cellebrite to discuss how CCTV and Home surveillance systems are assisting law enforcement with their investigations. Today more than 80% of cases involve video and require data correlation with mobile devices. Learn the best ways to access, review and analyze video in your investigations.

Target Level: All Levels
Target Audience: Government, Law Enforcement/Police, Corporate/Private Sector

Heron

Simplify Forensic Imaging: Bootable Forensic Imager and New Features on Ditto
Greg Dominguez, Digital Forensics Consultant, CRU

The demo highlights the new DittoX86, a bootable device that prepares a computer system for forensic imaging. This device eliminates the need to disassemble the computer to remove the hard drive. The presenter will also present new features on the Ditto and Ditto DX Forensic FieldStation imagers.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Monday, June 3 (continued)

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management · Forensics · Information Security · Investigations · Cellebrite Lab · Magnet Forensics Lab · Sponsor Demo

1:30pm – 2:20pm (continued)

Osprey

Optimizing Mobile Data Acquisition + Analysis with New XRY + XAMN Advancements
Jacob Hulsey, Director of Customer Success, MSAB

With the rapid development and adoption of mobile devices and the sheer volume of online communications, law enforcement agencies are often playing catch up when it comes to extracting and reporting on mobile evidence in a reliable manner. This session will show you the latest exploits for extracting data (app downgrade, Android Pi dumper, etc.) and how to import multiple file formats (.ufdr, .bin, GrayKey, Android Backup, etc.) into XAMN for analysis. You will learn how search, filter and report that data quickly using customizable profiles based on your investigation.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

3:30pm – 4:20pm

Oleander A

Case Study: Three Letters Company Delivering Valuable Information Via Email and How We Can Hack It.
Ondrej Krehel, Founder and CEO, LIFARS LLC
Pedro Freitas, Red Team Operator, LIFARS LLC

This session will share a case study demonstrating the dangers of sending personal and financial information via email and how criminals could exploit it, and how they in fact did it. During this session, the presenter will go over the steps of: Why it's not a good idea to send financial or personal information via email - in plain text; How criminals could exploit it for profit; and Lessons to be learnt.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Oleander B

IoT Wireless Network Forensics
Mike Raggo, Chief Security Officer, 802 Secure, Inc.

Current attack vectors indicate that nefarious attacks are increasingly targeting IoT wireless infrastructures throughout Cyber and Physical networks. Yet most organizations lack a defense-in-depth strategy to address the growing wireless threat landscape consisting of a plethora of new protocols and frequencies including: Wi-Fi, ZigBee, Z-Wave, Bluetooth, P25, M2M communications, and more. Since 80% of IoT is wireless across IT, OT, and IIoT; it's important for organizations to start designing an incident response and forensics strategy to address this growing risk of drones, spy cameras, Shadow IoT, rogue cell towers, Smart TVs, wireless storage devices, and much more. In this session, the presenter will explore the anatomy of these attacks to create a new foundation for IoT network threat detection and forensics.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Tides 1/2

Discover Vehicle Data: Vehicle Infotainment & Telematics System Forensics
Ben LeMere, CEO, Berla Corporation

A modern-day vehicle typically has 50-70 electronic control units (ECUs) or computers running on five different networks. User and vehicle data can be stored on these ECUs that can help investigators determine how a vehicle was operated, where it has been and who has been in the vehicle. With continued consumer demand of these sophisticated infotainment and telematics systems, the forensic benefit lies in the storage. All of this data can be critical evidence in an active investigation. This session will include: A comprehensive overview of what data can be acquired from infotainment and telematics systems within the vehicle; An in-depth discussion on the non-destructive methods to acquire and analyze it; and Real-life case studies at local and national levels.

Target Level: Beginner
Target Audience: Government, Investigators, Law Enforcement/Police

3:30pm – 4:20pm (continued)

Atlantic 3

Understanding the NIST Risk Management Framework

Denise Tawwab, Information Security Risk and Compliance Consultant, MLW & Associates

The NIST Risk Management Framework (RMF) is a 7-step process that you can use to architect and engineer a security program for your IT systems and data. Though not prescriptive, the RMF suggests best practices your organization should follow to identify, categorize, and secure your information systems and to protect your data. This session will take the mystery (and fear) out of how an information security program is established. It will clarify roles and responsibilities and give you a number of steps to take to ensure that your systems are secure, your data is protected, and your clients' privacy is maintained. At the end of this session attendees will: Understand the fundamental NIST Risk Management Framework principle; Know EXACTLY where to begin to establish your new information security program; Know how to identify gaps in your existing information security program; Understand the roles and responsibilities involved in an Information Security program; Have a solid foundation on which you can justify, prioritize, and build your data security strategy; and Leave with actionable "Next Steps" and a list of resources to move you forward.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Prosecutors/Attorneys/Legal

Atlantic 2

Cloud Forensics for Law Enforcement: Get the Evidence You Need to Move Cases Forward

Jamey Tubbs, Director, Training Operations, Magnet Forensics

Hands-On Lab: Evidence stored in servers belonging to service providers like Facebook and Google can be crucial in a law enforcement investigation and also among the hardest to acquire. Even when you can get a warrant to force a provider to return data, collecting the data into a normalized, easy-to-analyze format can be tricky. This lab will focus on Facebook's warrant return support and download your information features for both Facebook and Instagram. The presenter will describe how to ingest data into AXIOM Cloud and use commercial innovations to save time during investigations. The presenter will also discuss how to acquire photos from Twitter without requiring user credentials, and features such as Magnet.AI that can help you identify key pieces of evidence.

Target Level: Intermediate
Target Audience: Government, Law Enforcement/Police

Monday, June 3 (continued)

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management · Forensics · Information Security · Investigations · Cellebrite Lab · Magnet Forensics Lab · Sponsor Demo

3:30pm – 4:20pm (continued)

Atlantic 1

UFED Premium – The Only On-Premise Solution for Both iOS and Advanced Android Devices
Brian Stofik, Technical Forensic Specialist, Cellebrite Advanced Services
Joe Raspante, Administrator and Technical Forensic Specialist, Cellebrite Advanced Services

Come see the power of Cellebrite as we unveil our on-premise iOS and Advanced Android solution. As part of our Digital Intelligence Platform, this demo will share how you can unlock and extract iOS data to accelerate your investigations

Target Level: All Levels
Target Audience: Law Enforcement/Police

Heron

Crime Scenes to Courtroom – Processing, Investigating and Presenting Digital Evidence From All Sources To Show The Big Picture In A Holistic View
Robert O'Leary, Head of Investigations USG and Corporate, Digital Investigations SME, Nuix

Investigators are under increasing pressure to respond to challenges that the wide range of digital evidence sources and the diverse range of digital devices presents. In addition to laptops, computers and mobile devices, today's sources of digital evidence include network shares, Cloud Storage, IoT and more. Traditional digital forensic workflows often prevent an investigator from efficiently dealing with Big Data challenges. Key facts are often spread across multiple evidence sources and an investigation is typically multi-dimensional encompassing multiple people, objects, locations and events. Investigators need more efficient workflows to strive for Intelligence Driven Investigations that harness the power of big data, rather than becoming swamped by it. This includes collaboration across geographic and jurisdictional boundaries, sharing of intelligence and being able to identify hidden connections across large numbers of evidence sources.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Osprey

Grayshift & Magnet Forensics: Slaying iOS Investigations
David Miles, Co-Founder, Grayshift
Christopher Vance, Manager, Curriculum Development, Magnet Forensics

Investigating iOS devices has been a challenge for the mobile forensics industry for quite some time. Apple has continuously restricted or limited access to their devices over the past few years claiming user privacy trumps lawful access. Mobile forensics has always had two major challenges, acquisition and analysis. Getting to the data on iOS devices has always been a problem, and then once you're able to obtain the data, presenting it in a meaningful way is important especially when presenting it to non-technical stakeholders. With exciting and new extraction methods from Grayshift's GrayKey tool, and in-depth analysis with Magnet AXIOM of the most relevant data, iOS devices can become a valuable source of evidence for your investigations once again. Join Magnet Forensics & Grayshift to learn how GrayKey and Magnet AXIOM can be used together to get the most out of your iOS investigations, and be ready to revive some older cases and devices that were previously thought inaccessible.

Target Level: All Levels
Target Audience: Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

4:30pm – 5:20pm

Oleander A

Internet of Everything
Lee Reiber, Chief Operations Officer, Oxygen Forensics

Virtually every electronic in our lives can be connected to the Internet. What are the security risks of having so many devices connected? This session will identify vulnerabilities your company may not have already accounted for.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

4:30pm – 5:20pm (continued)

Oleander B

APFS Imaging Considerations for Forensic Examiners
Jason Roslewicz, CEO, Sumuri LLC

This session will address Privacy features built into Apple's newest Operating System, identify unique OS artifacts, and discuss acquisitions/system configuration of Mac OS Mojave systems.

Target Level: Beginner
Target Audience: Law Enforcement/Police

Tides 1/2

Integrating Cyber Threat Intelligence Into Your Security Team and Your Organization: Not Just Another Open Source Intelligence How To
Kall Loper, Director, National Lead for Incident Response, Protiviti
Mike Lefebvre, Associate Director, Protiviti

Cyber Threat Intelligence (CTI) can be invaluable to incident response, Security Operations Center (SOC) activities, and general information security. However, there is often a disconnect between CTI tasks and organizational structure. CTI analysts tend to operate as adjuncts to other functions (dotted line on organizational charts) or simply fill-in another title. This session examines the actual work produced by CTI within the scope of the organization's mission. The session will also share how CTI is integrated with a SOC/IR Team model using a Crisis Management-based IR Plan methodology as well as formalize the natural fit for CTI observed in many client security teams over the last several years.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government

Atlantic 3

Rapid Triage & Digital Investigations on iOS, Android, Mac, Windows, & More
Richard Frawley, Digital Forensic & Training Specialist, ADF Solutions

This session will share how to decipher if a case involving mobile or other digital devices require a full forensic examination and how to determine if the information at hand can get us to a successful outcome sooner. The presenter will discuss how investigators can exploit digital evidence to make rapid decisions based on "low-hanging fruit" and the pros and cons of using an automated triage approach to digital evidence collection, analysis and reporting.

Target Level: Beginner
Target Audience: Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Atlantic 2

Supporting the Unsupported: Carving, Parsing, and Creating Custom Artifacts
Christopher Vance, Manager, Curriculum Development, Magnet Forensics

Hands-On Lab: Many of the new mobile applications that daily hit the App Store and Google Play contain features that can contain crucial evidence. Often, though, commercial forensic tools cannot keep pace with these apps or their consumer usage. This lab will describe how to acquire evidence from a wide range of smartphones including Samsung, LG, Qualcomm, and off-brand devices using MTK chips. The presenter will review methods to discover and parse data from unsupported applications, including the chat, contact, location, and historical data that can be found using AXIOM's Dynamic App Finder. Finally, the presenter will discuss how to create custom artifacts to parse and carve data from the unsupported databases.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Law Enforcement/Police

Atlantic 1

Understanding Qualcomm's EDL Mode
Justin Cole, Manager of Contractors for Special Projects, Cellebrite
Keith Leavitt, Senior Trainer Developer, Cellebrite

Hands On Lab: From accessing data from damaged and non-functional Android devices, to extracting data from Android devices that are encrypted and locked, Qualcomm's Emergency Download Mode empowers examiners with an additional means for accessing Qualcomm chipsets that can be found on numerous Android Operating System mobile devices. This unique lab will walk attendees through a hands-on experience utilizing the Emergency Download Mode (EDL extraction method) for certain types of Qualcomm chipsets. Corroborate digital evidence located on mobile devices that is also stored in the Cloud.

Target Level: Intermediate
Target Audience: Government, Law Enforcement/Police, Corporate/Private Sector

Tuesday, June 4

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management | Forensics | Information Security | Investigations | Cellebrite Lab | Magnet Forensics Lab | Sponsor Demo

8:00am – 9:00am

Oleander A/B — **Early Riser Session: Dark Web, Version 2: The New Challenge for LE**
Stephen Arnold, Commissioner, International Tribunal for Justice

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.

Target Level: Intermediate
Target Audience: Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal, Corporate/Private Sector

9:30am – 10:20am

Oleander A — **Finding the Hidden Evidence on iOS and Android Devices**
Christopher Vance, Manager, Curriculum Development, Magnet Forensics

Increasing public scrutiny around the privacy implications of mobile OSes like iOS and Android means that changes will come to those OSes to meet customer demand. Those changes will make it harder to gain access to evidence on iPhones and Android devices that could potentially save lives and close cases, so digital investigation teams need to be on top of the latest changes to get the evidence they need. Join one of our mobile forensics experts to learn the best ways to get the most data from recovered devices.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Law Enforcement/Police

Oleander B — **We've Been Robbed! Understanding Adversary Exfiltration Techniques**
David Vargas, President, VATG, Inc.

The unfortunate fact is that most organizations will be compromised -- and after being compromised attackers will successfully exfiltrate stolen data. The methods used to remove this data are usually surreptitious, and sometimes clever. For example, several years ago attackers were able to successfully exfiltrate stolen data via a hacked smart fish tank. More recently, researchers proved that smart bulbs could be used to steal data. Since the techniques used are so varied, cyber defenders should be familiar them to be able to better detect and mitigate them. In this session attendees will learn: The most common techniques used to exfiltrate stolen data; The role of compression and encryption to obfuscate data; Why data exfiltration may occur only at certain times of day; How exfiltration is conducted on an air-gapped network; How data exfiltration is performed over C&C channels; and How and why adversaries use mediums other than the C&C channel to steal data. The presenter will also share why adversaries usually exfiltrate data in fixed size chunks and limit packet sizes and tow data exfiltration is performed with protocols that are different from the main C&C protocol or channel. After this session, attendees will be better able to better detect data exfiltration attempts and, as a result, will be better prepared to defend their networks.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

9:30am – 10:20am (continued)

Tides 1/2

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

Katherine Helenek, Senior Forensic Examiner/eDiscovery Specialist, Digital Intelligence

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.

Target Level: All Levels
Target Audience: Investigators

Atlantic 2

Finding the Best Starting Point for Insider Threats and Other Workplace Investigations

Trey Amick, Foresics Consultant, Magnet Forensics

More than half of data breaches reported by organizations are insider incidents either through the inadvertent or the malicious misuse of data. As enterprises expand the use of cloud-based services like SharePoint, Box, Dropbox, and Office365, they need to have a defined process and appropriate detection/investigative technologies to stay secure. During this demo, the presenter will look into the most common practices when conducting corporate investigations. Workplace investigations are rarely straightforward, as examiners, HR, legal and compliance professionals, you need to efficiently recover data to protect company assets. We'll explore how to find the best starting point for investigations like insider threats, employee misconduct and IP theft. From there, we'll highlight the benefits of an artifact first approach including: Filesystem artifacts relevant to corporate investigations; Simplify and expedite memory analysis with Volatility; Prove intent by visualizing relationships between files and actions; and Access employee cloud accounts with administrator credentials.

Target Level: Intermediate
Target Audience: Corporate/Private Sector

Heron

Managing the Changing Dynamic of Digital Forensics

Nick Drehel, Director Digital Investigations Training, AccessData

Mobile device investigations are growing exponentially. The number of mobile phones being examined has increased nearly tenfold over the past decade. Containing everything from text messages, call logs, contacts, internet history, email, and geolocation information embedded in photos, a mobile device can be a treasure trove of evidence crucial to an investigation, to help identify the who, what, when and where a crime was committed. Often investigations require separate tools for mobile and computer data analysis, driving up cost and wasting critical time. Investigators need a review platform that can bring all of this together. During this session, attendees will see how Quin-C from AccessData allows investigators to analyze computer and mobile data side-by-side for more streamlined investigations. With Quin-C, you can group email and text messages together and utilize powerful visualization tools to view similar data by social groups, identifying connections and possible accomplices. Plot mobile device photos on a map to place suspects at or near an event. And link multiple cases together with cross-case analysis capabilities. For even the most challenging caseloads, Quin-C can help accelerate the investigative process and maximize outcomes, in spite of growing data sets and shrinking budgets.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Osprey

EnCase Forensic + Tableau: Powerful Solutions for the Entire Digital Forensic Investigation Lifecycle

Jeff Hedlesky, Forensic Evangelist, OpenText, Inc.

To securely triage, acquire, investigate, and report the findings of your digital investigations, you must have the right combination of forensic hardware and software at your disposal. OpenText™ EnCase™ Forensic and Tableau hardware solutions are the market leaders in this domain and have been the tools of choice for thousands of field agents, lab technicians, and investigators for well over a decade. This informative demo session with experts from the OpenText EnCase & Tableau teams, will share the latest trends in digital forensics and how our compelling solutions can help address the challenges faced in today's digital forensic investigations. The presenters will talk about our unmatched encryption support, logical imaging, Apple File system (APFS) support, mobile forensics, acquisition from cloud, multi-language tool capability and much more. Be sure to bring your questions.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Tuesday, June 4 (continued)

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management **Forensics** **Information Security** **Investigations** **Cellebrite Lab** **Magnet Forensics Lab** **Sponsor Demo**

9:30am – 11:20am

Atlantic 3

The California Consumer Privacy Act & its Effect on the US Privacy Landscape

Harvey Nusz, Enterprise Architect and Manager, Privacy and Encryption+L92, Capgemini
Malu Milan, Lead Architect GRC-Risk Management-GDPR, Capgemini

This interactive session will focus on the California Consumer Privacy Act going into effect 01/01/2020, and any changes that occurred since its unanimous passing. The presenter will discuss: Key parts of GDPR and the NYDFS regulation; NISTS's efforts for a Privacy Framework and what that entails; The current efforts toward a national federal privacy law; and Key parts from other international privacy laws. The presenter will identify how to comply with Article 25, Privacy by Design to achieve Privacy by Default and the NYDFS regulation. After the session, attendees will leave with the knowledges to think about and consider how to implement Compliance on Demand, and how Privacy by Design, encryption and key management, and automating data subjects' rights fits into compliance on demand and combines to not only go far toward compliance, but also earn the trust of your customers, and differentiate your company from your competition.

Target Level: All Levels
Target Audience: Corporate/Private Sector

Atlantic 1

Carpenter vs USA – Understanding Reasonable Expectation of Privacy and the Proper Methods to Search and Seize Digital Data

Judge Mark McGinnis, Judge, State of Wisconsin

The United States Supreme Court held that individuals have a reasonable expectation of privacy in regards to their historical cell site location records that were collected from a third party. This session will discuss that decision and the impact it has on Fourth Amendment search and seizure issues, including the need to obtain a warrant to search or seize digital data.

Target Level: All Levels
Target Audience: Government, Law Enforcement/Police, Corporate/Private Sector

10:30am – 11:20am

Oleander A

Emoji: The Hidden Forensic Artifact?

Preston Farley, Special Investigator, Federal Aviation Administration

One of the most popular new ways people communicate in cyberspace today is via the emoji. This is particularly true in the mobile digital space. Studies have revealed that many young people communicate entirely through emoji. There is a blind spot in many of today's digital forensic examiners who are unaware of the proliferation of emojis as passwords and file names. This blindness may lead to the examiner missing critical evidence through sheer ignorance of modern glyph communication. There are also the forensic implications of using operating systems or forensic tools which do not support the latest available emoji characters. Even if the examiner is fully apprised of emoji usage, if their forensic tools don't support emoji decoding, this may also be crippling to an examination. Another issue regarding the use of emojis is that of the private use areas and private emojis. If suspects use these non-standard emojis, only the applications they were specifically created for may be able to decode them. This makes all an examiner's forensic tools effectively blind to private emoji communications. This session will discuss this passive form of crypto communication which could easily be overlooked by an examiner and is easily accessible by the average user. The presenter will share: Unicode implementation in computers-and why you should care; Emoji - Unicode linkage; Forensic consequences of emoji ignorance; and How to overcome them.

Target Level: All Levels
Target Audience: Investigators, Law Enforcement/Police

10:30am – 11:20am (continued)

Oleander B

So You Got Hacked; How Quickly Can your Company Recover?
Don Malloy, Chairman, Initiative for Open Authentication

This session will demonstrate where hacks are most successful, through hardware, software, firmware or the radio connected to the network. The hacking of IoT devices and systems will be explained in 6 basic steps. In addition, the presenter will discuss why protecting devices continue to be a challenging effort and how product vendors/developers and customers are all responsible for improving IoT device security. Lastly, the presenter will share the top 10 vulnerabilities.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Prosecutors/Attorneys/Legal

Tides 1/2

Legal Qualifications of a Testifying Digital Forensics Expert Witness in State and Federal Courts in Criminal or Civil Cases
Herbert Joe, Attorney/Board Certified Forensic Examiner, Yonovitz & Joe, L.L.P.; Law Office of Herbert Joe

Legal qualifications of any investigator, like a digital forensics examiner, to testify as an expert witness in state or Federal courts in civil or criminal cases have evolved since the landmark 1923 Frye case, as well as the more sweeping 1993 Daubert case, and continue to evolve, especially as technology advances. Although Rule 702 of the Federal Rules of Evidence have codified and standardized landmark Supreme Court cases (the "Daubert trilogy") for admissibility of scientific expert testimony in the federal courtroom (and most states by statutes), there are still "Frye states" with their own standards for admissibility of scientific expert testimony in their state courtrooms. This session discusses the important legal history of the qualifications, a general overview of different jurisdictional requirements, and the general requirements to testify as an expert witness in any digital forensics or cybersecurity case, or a checklist in legally challenging an opposing digital investigations expert in a Frye or Daubert pre-trial Hearing. Representative and recent case law will be discussed. So, whether your specialty is digital investigations, cybersecurity, attendees will learn about the practical aspects of becoming a testifying expert or challenging an opposing testifying expert, and be exposed to and discuss some relevant case law.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Tuesday, June 4 (continued)

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management **Forensics** **Information Security** **Investigations** **Cellebrite Lab** **Magnet Forensics Lab** **Sponsor Demo**

10:30am – 11:20am (continued)

Atlantic 2

Building a Timeline of User Activity Across Devices
Jamie McQuaid, Foresics Consultant, Magnet Forensics

Almost any type of investigation can benefit from timeline analysis to help understand what the user or the system did during a given incident. Whether you're trying to understand how a suspect distributed child exploitation material or are tracking malware pivoting across several systems in an intrusion, timeline analysis can help pinpoint the exact offense or step through exactly how an incident occurred. Join the presenter who will walk through a case using the new Timeline Explorer in Magnet AXIOM to show how timestamps can help tell a story in your investigation no matter if it's computer, memory, phone, or cloud data.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Law Enforcement/Police

Heron

Revolutionizing DFIR: Innovations, Advancements, and Game-Changing Technology for Investigators
Lee Reiber, COO, Oxygen Forensics

Technological advancements won't wait for investigators to catch up. If you are going to do your job, you need tools that push the envelope and keep you ahead of the curve. With the massive and ever-growing amount of data sources from mobile, IoT devices, and cloud storage services containing a multitude of images, messages, GPS data (and more!), investigators must have a solution to quickly triage, identify, and report. This session will give attendees a better understanding on how Oxygen Forensic Detective can be THE solution to their most critical investigations and how they can use it as a key source in solving difficult challenges in digital forensics.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police

1:30pm – 2:20pm

Oleander A

Introduction to Chip-Off Forensics
Jerry Diamond, Technical Trainer, MSAB

This session will provide attendees with an introduction into chip-off forensics. The presenter will share how to recognize and understand different chip designs, identify the correct chip for removal, and the proper technique for removing chips from circuit boards.

Target Level: All Levels
Target Audience: Investigators, Law Enforcement/Police

Oleander B

Malware Analysis and Reverse Engineering for Dummies
Luiz Borges, Consultant, TechBiz Forense Digital
Wilson Cordeiro, Consultant, TechBiz Forense Digital

This session will focus on introducing Malware Analysis and Reverse Engineering. The idea is to give the audience a broad understanding about the malware functionalities, the process of analysis and the reverse engineering of malwares. The presenter will show examples of known malwares and perform live analysis of the reverse code, discuss the impact of malwares in the digital scenario, discuss and propose automations to the analysis. The goal is to create a space for discussion and exchange of information for those that are starting in the malware analysis field. By the end, we hope that all the audience can perform a simple analysis and understand the process and the work that goes with this field.

Target Level: Beginner
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

1:30pm – 2:20pm (continued)

Tides 1/2

Extracting Data from Webpages and Social Media Using Free, Easy-to-Use Tools
Kevin DeLong, Founder and DFIR Researcher, AVAIRY Solutions

This session will share step-by-step how to use free tools and the Chrome web browser to extract data from webpages and social media accounts. You will learn how to load Chrome extensions and navigate the developer tools built in to Chrome. Finally, using a free, fully functional webscraper tool, you will learn how to select, capture, organize and extract to a CSV for your OSINT or Social Media Investigations.

Target Level: Beginner
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Atlantic 3

DHS Cyber Services and Protecting Critical Infrastructure
Klint Walker, Cyber Security Advisor, Department of Homeland Security

An overview of current threats and trends in Cyber Security along with an explanation of Cyber Services offered by DHS to assist critical infrastructure with defense strategies. Attendees will understand partnership opportunities and cyber programs available as voluntary services from the department.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Tuesday, June 4 (continued)

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management **Forensics** **Information Security** **Investigations** **Cellebrite Lab** **Magnet Forensics Lab** **Sponsor Demo**

1:30pm – 2:20pm (continued)

Atlantic 2

GrayKey and Magnet AXIOM: Bringing Platforms Together for Justice
Christopher Vance, Manager, Curriculum Development, Magnet Forensics
David Miles, Co-Founder, Grayshift
Mitch Kajzer, Cyber Crimes Director, Office of the Prosecuting Attorney, St. Joseph County

The combination of GrayKey and Magnet AXIOM has dramatically changed the way law enforcement conducts investigations on iOS devices. Just a short time ago, the statement, "I don't know the passcode" meant that it was likely the device would not be accessible and evidence crucial to an investigation would remain undiscovered. In this case study, participants will learn about the benefits of using the combination of Grayshift's GrayKey and Magnet Forensics' AXIOM and see how investigators went from having a locked iPhone and zero evidence to having an overwhelming amount of evidence against a suspect. This session is for law enforcement only.

Target Level: Intermediate
Target Audience: Government, Law Enforcement/Police

Atlantic 1

UFED Premium – The Only On-Premise Solution for Both iOS and Advanced Android Devices
Brian Stofik, Technical Forensic Specialist, Cellebrite Advanced Services
Joe Raspante, Administrator and Technical Forensic Specialist, Cellebrite Advanced Services

Come see the power of Cellebrite as we unveil our on-premise iOS and Advanced Android solution. As part of our Digital Intelligence Platform, the presenters will show attendees how to unlock and extract iOS data to accelerate your investigations.

Target Level: All Levels
Target Audience: Law Enforcement/Police

Heron

System Files Tricks for Forensic Investigation and Incident Response
Yuri Gubanov, CEO and Founder, Belkasoft USA

System files may tell you a lot about the user or malware actions on a computer or a laptop. They may give you a hint about deleted files, opened documents, computer reboot or malware persistence. This session will discuss what you can extract from Windows registry, event logs, Amcache/ShimCache/Syscache, BAM/DAM, AppInit DLLs, jumplists, Windows 10 timeline and remote connections data. With the help of the newest version of Belkasoft Evidence Center, you will be able to find important artifacts inside system files, which will help you to solve a forensic case or an incident response case. This session will be useful for both law enforcement and the private companies' investigators.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Investigators, Law Enforcement/Police

Osprey

New DATAPILOT 10 Field Triage Device: Acquire Immediate Evidence from Mass-Casualty Vvents
Jeremy Kirby, Director of Sales, Susteen, Inc.

Learn how to acquire immediate digital evidence in the field.

Target Level: All Levels
Target Audience: Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

3:30pm – 4:20pm

Oleander B

"Private" Browsing: Your Secret is Not Safe - Forensic Analysis of Private Browsing Mode Activity

Joe Walsh, MCJ Program Director and Instructor of Criminal Justice/Computer Science, DeSales University

Most modern web browsers offer private browsing modes, but how private are they? This session will review the privacy offered by these features. The presenter will discuss the results of research he conducted on the private browsing modes available in several popular web browsers. These results will help attendees to understand the level of privacy they are actually achieving when using private browsing mode. Best practices for forensic examiners will also be discussed, so that examiners can ensure they are obtaining all the evidence that might be available to them.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Tides 1/2

Cyber Supply Chain Security

Matthew Caldwell, CEO and Founder, Tophat Security Inc.

Cyber supply chain security is the identification of risks involving vendors, suppliers, partners and other related entities which can impact the security of your organization or products. Even though recent national and international news headlines have brought the topic to the forefront, this evolving threat landscape has been simmering for years and remains largely unaddressed. Blind faith is no longer an option! During this session, the presenter will: Explain the risks and potential impact to your organization or products; Discuss why the cyber supply chain security threat is all too real and share findings from years in the field; and Share practical solutions to supply chain security.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Atlantic 3

Auditing Cyber Defense Technologies

Speaker, Stephen Head, Director, Experis Finance

Auditing the many cyber defense technologies currently being deployed to defend organizations against cyber-attack is extremely challenging, whether your organization is public, private or governmental. In response to the growing frequency and severity of cyber-attacks, many organizations are implementing a new generation of security tools that did not exist just a few years ago. In this fast-paced session, the presenter will examine these new and emerging tools for defending against cyber-attacks, how they work, how they can be leveraged for continuous monitoring, who the leading players are, and how these technologies can be audited. Attendees will receive: An understanding of this new generation of cyber defense tools and how they work, so attendees can immediately get up-to speed on how these tools are changing the security landscape within their organization; Key success factors for deploying these tools that if ignored may lead to openings that can be exploited by attackers; and Techniques for leveraging these tools to facilitate continuous monitoring and extend audit coverage beyond what is currently attainable.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators

Atlantic 2

Thinking DFIRently: Utilizing Technology to Work Smarter Than Ever

Jessica Hyde, Director of Forensics, Magnet Forensics

We've passed the early stages of digital forensics. The early processes and methods that we initially developed still have their place, but technology has exploded past that point. This is the time to think outside the box and figure out how we're going to use the tools at our disposal to meet the challenges that are ahead of us. We need to think about what evidence is often missing — whether it's victim/witness evidence, Chromebooks, IoT, and the Cloud — and how we're going to integrate them into our investigative processes. How do we take all the possible evidence sources in front of us and utilize our expertise, all while working smarter, faster, and better?

Target Level: Intermediate
Target Audience: Government, Law Enforcement/Police

Atlantic 1

Leveraging Technology and AI to Expedite Investigative Efforts

John McHenry, Director Curriculum, Cellebrite

An in-depth analysis of how advanced analytics can improve your investigative process and why analytics is a required tool in today's digital investigations. With the increasing amount of data in the typical case, even the best investigator can find themselves at a crossroad. With advanced analytics you can reduce any amount of data to just the relevant facts.

Target Level: All Levels
Target Audience: Government, Law Enforcement/Police, Corporate/Private Sector

Tuesday, June 4 (continued)

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management **Forensics** **Information Security** **Investigations** **Cellebrite Lab** **Magnet Forensics Lab** **Sponsor Demo**

3:30pm – 4:20pm (continued)

Heron

xBit Digital Case Management: A Proven Lab Solution Designed for the Forensic Investigator and Managers
Nolan Tracy, Advanced Mobile Forensic Instructor/Project Director

Organize your digital forensic case data with xBit, the digital case management solution built to simplify the task of cataloging information unique to the digital forensic investigator.

Target Level: Beginner
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

3:30pm – 5:20pm

Oleander A

Overcoming Challenges with the Admissibility of Digital Evidence
Moderator: Judge Mark McGinnis, Judge, State of Wisconsin
Panelists: Ed Michael, Detective, Orlando Police Department
Richard Colangelo, State's Attorney, Judicial District of Stamford/Norwalk

During this interactive panel discussion, attendees will learn about common challenges that arise during judicial proceedings as to the admissibility of digital evidence. Panelists will share their experiences and offer insight on how to avoid legal pitfalls.

Target Level: All Levels
Target Audience: Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

4:30pm – 5:20pm

Oleander B

Identifying Darknet Suspects: When Law Enforcement Hacks
Searchlight Security

Increasingly, drug dealers and child abusers are using darknet anonymizing technologies to peddle their wares and collaborate with like minded individuals. In many cases, this entirely thwarts law enforcement's ability to identify them giving them free reign to act with impunity. However, in recent years we have seen a select few agencies using computer vulnerabilities in common software (e.g. Firefox) to gain remote code execution (RCE) on the suspect's computer and force it to identify itself. These techniques, often called Network Investigative Techniques (NITs), have been deployed in a small set of darknet investigations allowing the identification and arrest of thousands of high value suspects who would have previously remained hidden. In essence, except for their end goal, NITs are no different from tools deployed by cyber criminals. In this session, the presenter will give an overview through a series of case studies of the use hacking capabilities to remotely compromise computers operated by criminals and collect evidence. Attendees will learn: An overview of a series of international darknet investigations; How Network Investigative Techniques work at a technical level; and Legal complications around the use of NITs.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

4:30pm – 5:20pm (continued)

Tides 1/2

Putting the Intelligence Back in Threat Intel (Because Math)

Edward McCabe, Founder/Principal, The Rubicon Advisory Group

Threat Intelligence isn't about having a sea of honeypots, raw source feeds of bad IP addresses, domains & hashes, or log files — we already have that; it's about taking that data, turning it into information so we can make decisions and take action! Let's be honest, raw data is everywhere; truth is, we're drowning in it. We have the ability to collect data from almost everywhere on a near constant basis; however, the mere collection and retention of data does not mean we have "Threat Intelligence", it just means we're hoarding data. Analysis is required; only through analysis can we produce actionable intelligence and bring that business value to the table. This session will cover various methods available, when they are appropriate, and how they can be leveraged to help secure your organization and reduce risk. After completing this session, attendees will be able to: Understand the need for defined information requirements relating to threat intelligence; Improve their knowledge regarding how leveraging threat intelligence lowers risk to their organization; Better understand how a defined and consistent application of analysis techniques address the various risks (strategic, operational & tactical); and Better understand the business value that a properly implemented threat intelligence program brings to the organization.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police

Atlantic 3

Zip File Forensics

Blazer Catzen, President, Catzen Forensics

We all rely on date time stamps and believe that a windows created time is the time the file was born on that media. Files extracted by zip behave differently. For example PK zip file extraction will use the modified time for a created time when extracting to NTFS. This session will look at multiple archive utilities to understand both the file structure of the archive by utility (PKZip, WinZip, Windows native, 7Zip, etc.) as well as understand the behavior of file extraction date time stamping for multiple applications and multiple methods of extraction (extract v drag-drop). At the end of the session, attendees should have an understanding of the behavior as well as have a framework for the analysis and testing of any zip archive.

Target Level: Intermediate
Target Audience: Investigators, Law Enforcement/Police

Atlantic 2

Preserving Casework Integrity from Chaos: Using Magnet ATLAS

Kevin Harth, Customer Solutions Manager, Magnet Forensics
Luis Martinez, Criminal Investigator, Westchester County District Attorney's Office

Westchester County District Attorney's Office needed more with regard to tracking evidence, data, assets, and collaborating with non-technical stakeholders. They required a solution that understood the intricacies of forensic investigations, but could still bring all the elements of a case together for consistent, simple management. Join us for this case study to learn why they chose Magnet ATLAS and how it helped them create a clear chain of custody for evidence, manage cases, and how it allowed them advanced analytics and reporting capabilities for various stakeholders.

Target Level: Intermediate
Target Audience: Government, Law Enforcement/Police

Atlantic 1

Digital Transformation in Law Enforcement

Frank Toscano, VP of Product Marketing, Cellebrite
Brendan Morgan, Vice President of Training for the Americas, Cellebrite

This session will focus on 3 overarching strategy pillars that police agencies will need to implement to deal with the exponential growth of data as a response to current challenges facing police forces with the increase in technology-enabled crime.

Target Level: Intermediate
Target Audience: Government, Law Enforcement/Police, Investigators

Wednesday, June 5

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management **Forensics** **Information Security** **Investigations** **Cellebrite Lab** **Magnet Forensics Lab** **Sponsor Demo**

9:00am – 9:50am

Oleander A

Forensic Identification of Fake Digital Photos

Chet Hosmer, Author, Python Forensics, Inc.

The phenomena of Fake Photos, Audio recordings, and Video have become viral. Just one example according to the Washington Post (2017), "following an attack on the London Bridge that killed eight people, fake photos started popping up of individuals falsely labeled as missing. Internet trolls widely shared a grainy picture of a man driving a silver car and said it was a picture of the suspect. (It turned out to be an old photo of a controversial but unrelated American comedian.)" This activity has become commonplace on the Internet, and Social Media and the results in many cases end up on the nightly news as FACTS. Not only is this practice extremely dangerous and unethical but it is simply fraud.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Oleander B

How I Would Attack SQL Server

Brian Kelley, Infrastructure Architect, Truth Solutions, LLC

This isn't a talk about best practices or how to configure your system. It's designed to get into the mindset of a motivated, equipped adversary who wants to get in to a system or application, specifically SQL Server, and uses the full extent of his or her creativity to do so. This session will look at both traditional and non-traditional weak points, how an attacker discovers them, exploits them, and then covers up his or her tracks. The presenter will discuss what we can do to compensate for a weakness we can't fix, which revolves mostly around detection and response and how an attacker will respond to such countermeasures.

Target Level: Beginner
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police

Atlantic 2

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

Trey Amick, Forensics Consultant, Magnet Forensics

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. This session 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.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Law Enforcement/Police

Atlantic 1

Leading a Corporate Investigation: Acquisition Through Testimony

Clark Walton, Managing Director, Reliance Forensics, LLC

This session will walk through various technical scenarios of forensic investigations specifically as they relate to the theft of confidential or protected corporate information of a business entity. Emphasis will be placed on real-world scenarios and the effective role of the digital forensic examiner: from initial acquisition and reporting, to temporary restraining orders and preliminary injunctions, expert reporting and depositions in discovery, and finally effective testimony at trial.

Target Level: All Levels
Target Audience: Government, Law Enforcement/Police, Corporate/Private Sector

9:00am – 10:50am

Atlantic 3

Good Fences Make Good Neighbors - Auditing the CyberSecurity of Your Network DMZ

Ken Cutler, Principal Consultant, Ken Cutler & Associates, LLC

Today's Internet connections are typically shielded by a Demilitarized Zone (DMZ), a critical CyberSecurity buffer zone between your organization's internal network and the outside world. Firewalls, intrusion detection/prevention systems, proxy servers, load balancers, filtering routers, VLANs, and VPNs all play a major role in regulating and restricting traffic flowing to and from Internet CyberSpace. Failure to properly configure, maintain/patch, and monitor a secure and efficient DMZ increases the risk of your organization being attacked by CyberCriminals and other external intruders. This intensive seminar is designed to help your organization develop an effective, comprehensive audit plan to test your network's perimeter CyberSecurity both internally and externally. The presenter will discuss: Developing a DMZ and Network Perimeter Cybersecurity Audit Plan; Identifying the Control Points; and Tools, References, and Techniques for Auditing Network Devices and Perimeter Cybersecurity: Internally and Externally. Note: Basic understanding of TCP/IP network concepts by the attendees is assumed.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government

9:00am – 11:50am

Tides 1/2

Virtual Currency Investigations: Hands-On Lab and Lecture

Eric Huber, Vice President, National White Collar Crime Center (NW3C)

Cryptocurrencies used extensively as key payment method of the underground economy and to facilitate many other forms of criminal activity including money laundering, child exploitation, and ransomware. Proficiency in understanding and investigating cryptocurrencies and their underlying blockchain technology is no longer optional for cybercrime investigations. This introductory hybrid lecture/hands on lab presentation assumes no prior knowledge on the part of attendees. This session will educate attendees on key blockchain technology concepts such as distributed ledgers, mining, public key cryptography, and blockchain wallets. Concepts such as privacy coins and stable coins will be covered along with the uses of blockchain technology beyond cryptocurrency such as the facilitation of distributed applications (DAPPS) and Internet 2.0. The second half of the session will focus on the ever expanding criminal uses of cryptocurrencies and how they can be successfully investigated with both free and paid tools using a comprehensive virtual currency investigation process that includes digital forensics, open source investigations, and traditional investigative methods. The session will conclude with providing students how they can plug into the cryptocurrency community and begin their own path to education and exploration of this financial technology that will be a key part of cybercrime investigations for a very long time to come.

Target Level: Beginner
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

10:00am – 10:50am

Oleander A

Windows® 10 Timeline Forensic Analysis

Rob Attoe, CEO, Spyder Forensics, LLC

The Windows 10 April 2018 update (1803) introduced a new feature named "Timeline" which has been further enhanced in subsequent updates to the Operating System in late 2018 and early 2019. This feature acts like a browser for all your recent file and web interactions on the local computer and if enabled your additional trusted devices too. It provides a chronology view of interactions, which not only contains the websites visited but all documents you opened or edited, the pictures you viewed and games you played as well as information of which machine it was interacted with. This session will take a deep dive into the artifacts this feature creates and how they may be used by the system and interpreted in a forensic examination. Attendees will gain a deeper understanding of the complexities of this feature and a first hand look at the SQLite database containing all the artifacts and understanding of the cloud based synchronization issues.

Target Level: Advanced
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police

Wednesday, June 5 (continued)

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management | Forensics | Information Security | Investigations | Cellebrite Lab | Magnet Forensics Lab | Sponsor Demo

10:00am – 10:50am (continued)

Oleander B

Cyber Security Considerations for Small and Medium Businesses

Marc Laliberte, Senior Security Analyst, WatchGuard

US small businesses contributed over half the total $17 trillion GDP, and yet at least 61% of small to medium businesses have seen a cyber-attack and 60% of them go out of business within a year after an incident. Cyber security is a critical issue for this sector, the economy, and our nation. Learn the latest trends and understand the information technology security considerations that will impact small and medium business in 2019. Hear stories from the front line of small and medium business organizations across the globe, understand the critical considerations from 2018 small business cyber security threat research trends, and decide for yourself what SMB's should be preparing for, and how it will also impact your business in 2019.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Prosecutors/Attorneys/Legal

Atlantic 2

Android Virtualization with MAGNET App Simulator

Jamie McQuaid, Foresics Consultant, Magnet Forensics

While the recovery of essential data from your evidence is paramount, presenting that data can be just as important. Examiners are used to looking at raw, unstructured data to piece together valuable evidence but when it comes to presenting to stakeholders, especially non-technical ones, it's best to show the data as close to the user's view as possible so that they can best understand the user's intentions. Visualizing this data isn't always easy, especially on a mobile device. MAGNET App Simulator gives visualization to Android applications found during your investigations. Allowing for the examiner to load application data from Android devices in your case into a virtual environment, MAGNET App Simulator enables you to view and interact with the data as the user would have seen it on their own device. This session will introduce MAGNET App Simulator as a free tool for examiners to visualize Android app data and show how it can be used in your investigations.

Target Level: Intermediate
Target Audience: Corporate/Private Sector, Government, Law Enforcement/Police

Atlantic 1

Cloud Forensics for Your Investigation

Justin Cole, Manager of Contractors for Special Projects, Cellebrite
John McHenry, Director Curriculum, Cellebrite

Learn about Cellebrite's UFED Cloud Analyzer and how you can use it to recover forensically sound content, from more than 40 cloud applications and sources. This session will describe how to export an account package and how to ingest it into UFED Cloud Analyzer. The presenters will show how to use the password collector to retrieve credentials saved on mobile browsers and apply them in the product to retrieve cloud data. In addition, the presenters will review features like Web Capture, getting public data in UFED Physical Analyzer and how to apply an iCloud Backup when an actual device is not available. The session will also walk through best practices for acquiring cloud warrants.

Target Level: All Levels
Target Audience: Government, Law Enforcement/Police, Corporate/Private Sector

LOOK DEEPER WITH BELKASOFT

Belkasoft
forensics made easier

VISIT OUR BOOTH #216

TALK TO BELKASOFT TO KNOW MORE ABOUT

BELKASOFT EVIDENCE CENTER

ALL-IN-ONE DIGITAL FORENSIC TOOL SUPPORTING MOBILE, COMPUTER, RAM, CLOUD AND REMOTE FORENSICS.

ATTEND OUR PRESENTATIONS:

Secret Deal!

June 2 (Sunday) 4:00pm - 4:50pm
Telegram Messenger Investigation on Mobile Devices

June 3 (Monday) 10-30am – 11-20am
SQLite forensics and **Memory** forensics with Belkasoft Evidence Center, all-in-one forensic solution

June 4 (Tuesday) 1:30pm – 2:20pm
System files tricks for forensic investigation and incident response

Wednesday, June 5 (continued)

The 2019 Conference Program is defined by primary topics. Please use the color legend below to quickly identify the primary topic for each session. Target levels and target audiences have also been listed to help attendees select the best sessions for individual needs/experience, but by no means should exclude or deter anyone from attending a session of interest.

Audit/Risk Management **Forensics** **Information Security** **Investigations** **Cellebrite Lab** **Magnet Forensics Lab** **Sponsor Demo**

11:00am – 11:50am

Oleander A

Go-Go Gadget, Smartwatch! An Investigation of Wearable Devices & Their Forensic Value

Jess Lindmar, Forensic Scientist and Section Supervisor, Virginia Department of Forensic Science
Nicole Odom, Forensic Scientist Trainee, Virginia Department of Forensic Science's (DFS) Digital & Multimedia Evidence (DME)

After attending this session, attendees will have an enhanced understanding of how smartwatch wearable devices with cellular network capability interact with companion mobile phones and where sensitive user data and forensic artifacts are stored, both through utilization as a standalone and connected device. It will also provide a methodology for the forensically sound acquisition of data from a standalone wearable device. The results of a robust research project will be presented, as well as general observations made throughout the investigation and any future directions or recommendations.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Investigators, Law Enforcement/Police

Oleander B

Processing of Mobile Devices from Victims or Witnesses

Martin Novak, Senior Computer Scientist, National Institute of Justice
Sudhir Aggarwal, Professor, Florida State University
Gokila Dorai, Ph.D. Student, Florida State University

Existing law enforcement tools to collect evidence from mobile devices are designed based on the assumption that the device in question has been legally taken from the alleged perpetrator of a crime because of its potential evidentiary value. As a result, they are likely to capture all data held on a mobile device including data that are not germane to the incident in question. Law enforcement needs the capability to collect digital evidence from victim or witness devices discriminately — where broad capture of all data might capture data that are not relevant to the case being investigated. Protection of the privacy of data from witness and victim mobile devices that are not appropriate to the incident is paramount in this instance. This session will share a new technology for processing mobile devices from victims or witnesses — Targeted Forensic Data Extraction from Mobile Devices (TFDEMD).

Target Level: Intermediate
Target Audience: Investigators, Law Enforcement/Police, Prosecutors/Attorneys/Legal

Atlantic 3

Risk Management Framework (RMF) Implementation: A Real World Analysis

James Dodmead, U.S. Navy IT Specialist, U.S.Navy, Naval Information Warfare Center, Atlantic

Are you worried about the cybersecurity posture of your system, but not sure that you can sit through another dry RMF presentation? This may be just what you are looking for. The advent and implementation of RMF has resulted in a lot of angst within both military and government cybersecurity communities. Estimates are that RMF implementation is 400 to 800% more difficult than the previous process, depending on the sensitivity of the system and the associated timeline. While RMF is much more granular than the previous Department of Defense (DoD) system, the question remains as to its worth as opposed to the increased effort required. After sitting through one too many vague, dry RMF presentations, the presenter seeks to portray RMF in a more realistic light. The speaker will begin with a brief overview of the six step RMF process. This will be followed by a review of recent newsworthy cybersecurity incidents and how proper RMF implementation could have helped to prevent them.

Target Level: All Levels
Target Audience: Corporate/Private Sector, Government

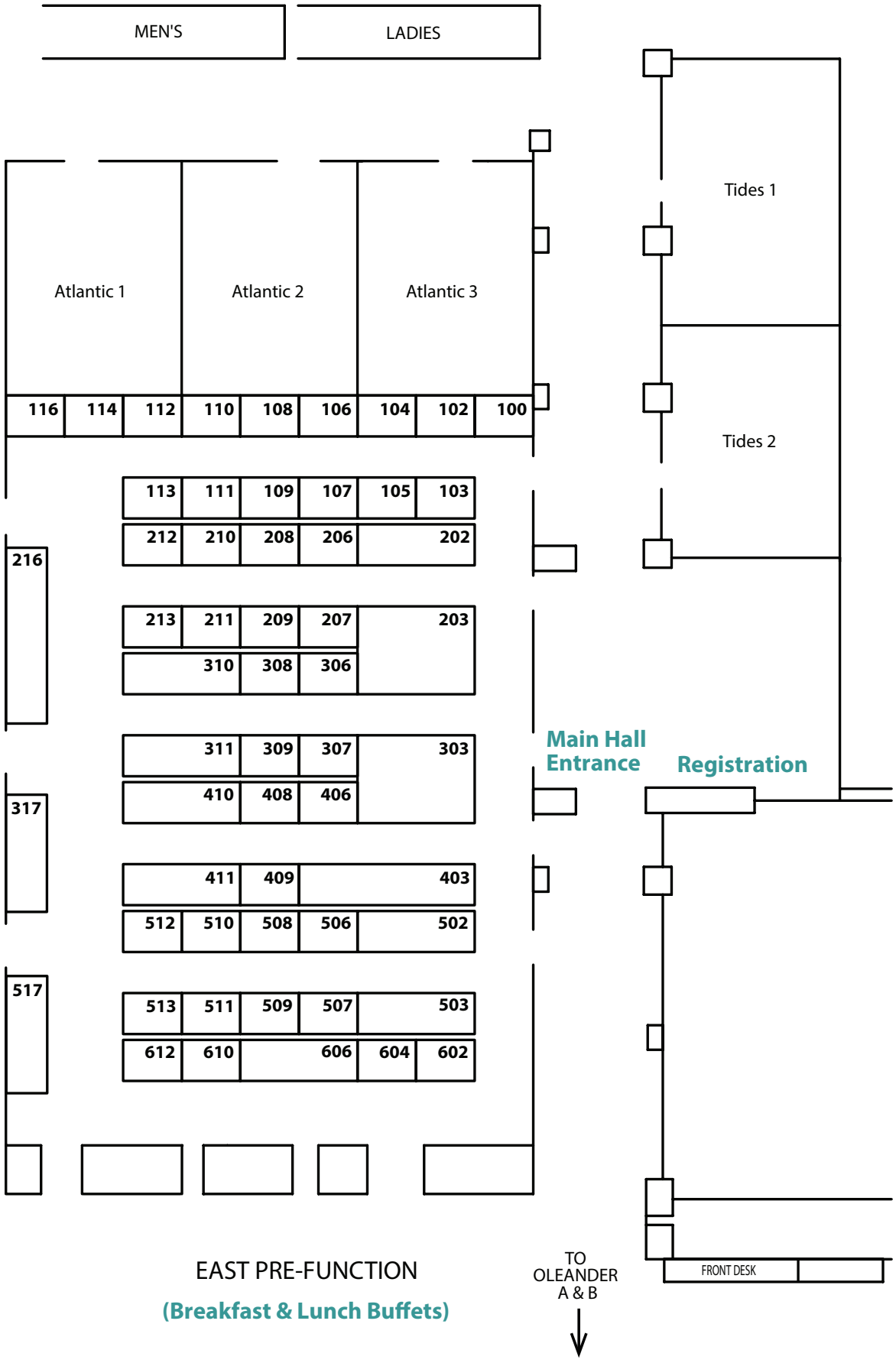
Atlantic 1

Leveraging Technology and AI to Expedite Investigative Efforts

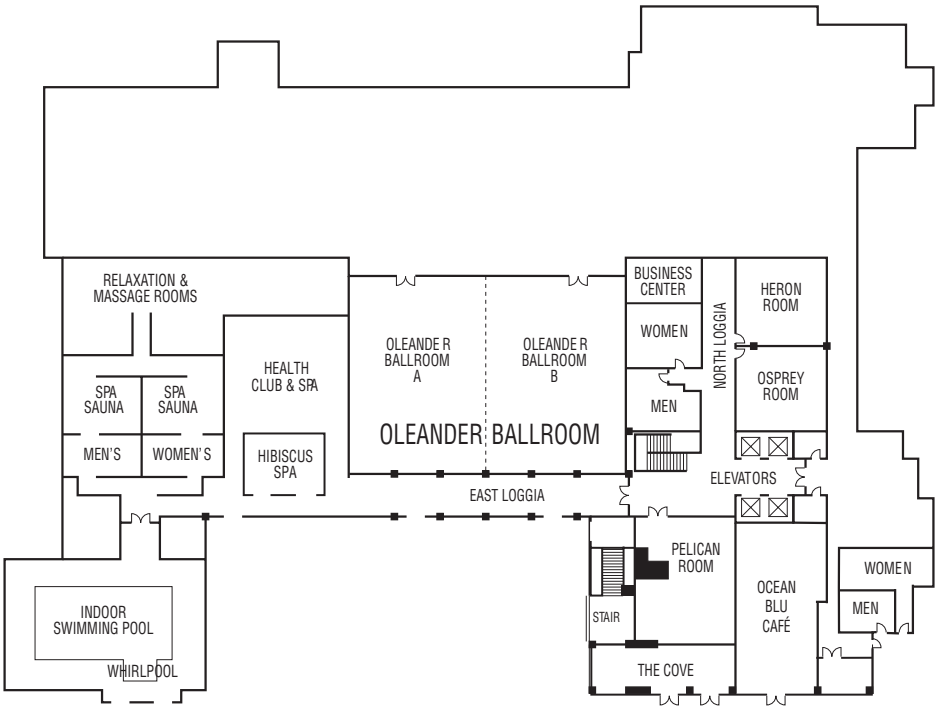
John McHenry, Director Curriculum, Cellebrite

An in-depth analysis of how advanced analytics can improve your investigative process and why analytics is a required tool in today's digital investigations. With the increasing amount of data in the typical case, even the best investigator can find themselves at a crossroad. With advanced analytics you can reduce any amount of data to just the relevant facts.

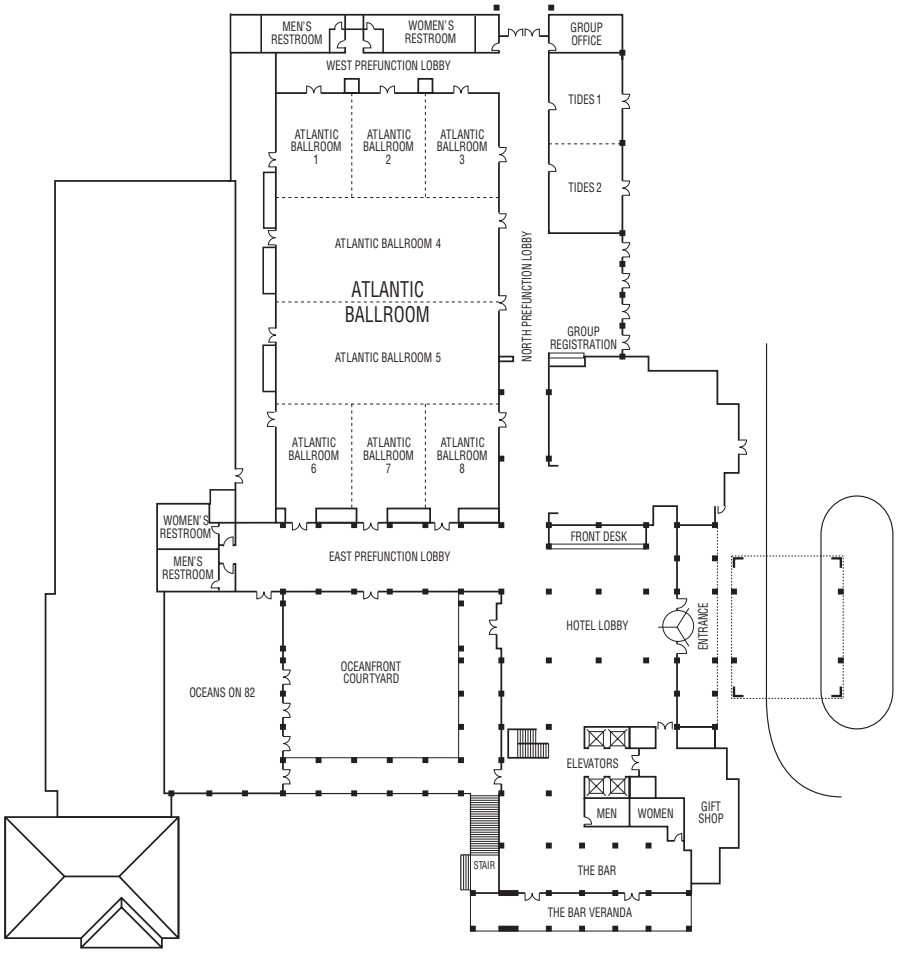
Target Level: All Levels
Target Audience: Government, Law Enforcement/Police, Corporate/Private Sector



LOWER LEVEL



MAIN LEVEL



AccessData

Booth 202

Lindon, UT, USA
(513) 806-7391

www.accessdata.com

AccessData® offers industry-leading solutions that put the power of forensics in your hands. For 30 years, we have worked with more than 130,000 clients in law enforcement, government agencies and corporations around the world to focus on their unique collection-to-analysis needs. The result? Faster results, better insights, and more connectivity.

ACE Lab

Booth 513

Prague, Czech Republic
+420 222 361 605

www.acelab.eu.com

ACE Lab is internationally recognized as a pacesetter in the development of the most comprehensive solutions for recovering data and evidence from the widest range of storage devices. For 27 years data recovery engineers and digital forensics experts from over 117 countries have been awarding their trust to PC-3000.

Ace Technology Partners

Booth 116

Elk Grove Village, IL, USA
(847) 952-6900

www.acetechpartners.com

Ace Technology Partners is a 36 year ISO9001:2015 certified System-Integrator who focuses on Digital Forensic investigations. We work in local, state, federal and international markets and hold multiple contracts including NASPO-Valuepoint, NASA SEWP_V, Air Force NetCents2 and others. Come and see our latest FORCE™ Workstations and CipherFORCE™ Password Cracking Appliances!

ADF Solutions

Booth 309

Bethesda, MD, USA
(301) 312-6578

www.adfsolutions.com/free-trial

ADF makes the best digital forensic and media exploitation tools for law enforcement. These tools are used for processing and analyzing smartphones, mobile devices, computers, external drives, drive images, and other media storage (USB flash drives, memory cards, etc.). Schedule a demo or request an evaluation at www.tryadf.com.

Argent

Booth 100

Chapin, SC, USA
(704) 298-8086

www.Argent.com

Argent's Advanced Technology (AT) is a highly scalable, feature-rich and mature monitoring tool. AT's discovery process is accurate, its thresholds can express sophisticated networking situations and it can flexibly send alert notifications to multiple administrators. AT can automatically correct a wide range of network problems.

Atola Technology

Booth 114

Surrey, BC, Canada
(888) 540-2010

www.atola.com

FAST FORENSIC IMAGING, EVEN WITH DAMAGED DRIVES! Get more digital evidence faster with INSIGHT FORENSIC and TASKFORCE Forensic Imagers. The first and only forensic data acquisition tools that can get data from both good and even damaged hard drives and they are one-button simple to use!

AVAIL Forensics

Booth 102

Wilmington, NC, USA
(877) 888-5895

www.availforensics.com

"Turning Case Evidence into Case Intelligence". AVAIL Forensics, formed in 2006 with the mission of serving the computer forensics community offering a wide spectrum of custom hardware and field triage kits. AVAIL, the Original and Only TRUE Custom-Built DF-Hardware and DOMEX Kit provider creating our "DAVE" line. "Justice through Technology".

Belkasoft LLC

Booth 216

Palo Alto, CA, USA
(650) 272-0384

www.belkasoft.com

Belkasoft is a global leader in digital forensics, known for their sound and comprehensive forensic tools. With a team of professionals in forensics, data recovery and reverse engineering, Belkasoft focuses on creating technologically advanced yet easy-to-use products for investigators and experts to make their work easier, faster, and more effective.

Berla

Booth 111

Annapolis, MD, USA
(443) 333-9301

www.berla.co

Berla is leading the way in vehicle forensics technology, enabling the acquisition and analysis of user data stored in vehicle infotainment and telematics systems. Berla's ecosystem of forensic tools support investigators throughout the entire process to identify, acquire, and analyze vehicle data.

BlackBag Technologies

Booth 213

San Jose, CA, USA
(408) 844-8890

www.blackbagtech.com

Blackbag Technologies develops innovative forensics acquisition, triage, and analysis software for Windows, Android, iOS, and Mac OS X devices and creates industry-leading digital forensic training courses for everyone from novice to experienced investigators. Our courses and software are trusted by hundreds of federal, state, and local law enforcement agencies worldwide.

Cellebrite

Booth 303

Parsippany, NJ, USA
(973) 206-7756

www.cellebrite.com

As the global leader in digital intelligence with more than 60,000 licenses deployed in 150 countries, Cellebrite provides law enforcement, military and intelligence, and enterprise customers with the most complete, industry-proven range of solutions for digital forensics, triage and analytics. Cellebrite: providing digital intelligence for a safer world.

Cobwebs Technologies

Booth 103

New York, NY, USA
+972 58-4444632

www.cobwebs.com

Cobwebs Technologies is a global leader in Web Intelligence. Our innovative solutions are tailored to the operational needs of national security agencies and the private sector, identifying threats with just one click.

CRU

Booth 310

Vancouver, WA, USA
(360) 816-1751

www.cru-inc.com

CRU's line of WiebeTech digital forensic devices are used to procure and preserve data to use as evidence of wrongdoing or malicious intent. These devices are used by security teams, criminal investigators, discovery personnel, and by the military and other government agencies.

Cyan Forensics

Booth 106

Edinburgh, Scotland, United Kingdom
+44 131 608 0195

www.cyanforensics.com

Cyan Forensics provides software to find evidence on computers many times faster than before, doing in minutes what can currently take days. Cyan Forensics also helps to simply and securely share the data that powers these searches, especially CSAM and material of interest in Counter Terrorism investigations.

DeSales University

Booth 307

Center Valley, PA, USA
(610) 282-1100

www.desales.edu

DeSales University offers degree and certificate programs in cybersecurity and digital forensics. Digital forensics prepares students to analyze digital evidence. Cybersecurity prepares students to become security professionals who can prevent and respond to security incidents while complying with applicable legal regulations. All classes are offered online and feature flexible schedules.

Digital Intelligence, Inc.

Booth 105

New Berlin, WI, USA
(262) 782-3332

www.digitalintelligence.com

Digital Intelligence is a privately held company founded in 1999 and known worldwide as a pioneer in digital forensic hardware. Today we offer a full array of products, forensics and e-discovery consulting services and customizable training. Our customers include law enforcement, government agencies, corporations and law firms in 100+ countries.

DME Forensics

Booth 308

Golden, CO, USA
(800) 413-0363

www.dmeforensics.com

DME Forensics is an innovative technology company focused on providing digital and multimedia evidence solutions to the criminal and civil justice communities. We develop technologies that assist investigators in a variety of cases, such as: terrorism, civil unrest, homicide, property crimes, and child exploitation.

EDEC Digital Forensics

Booth 207

Santa Barbara, CA, USA
(805) 222-4584

www.edecdf.com

Next-generation RF shielding — EDEC Black Hole™ bags are the original RF shielding products designed for digital forensic investigators, police, military and federal agencies. After 10 years, EDEC is again at the vanguard of evidence protection with the launch of Off Grid™, a product line with advanced features for a new generation of evidence security.

ELCOMSOFT

Booth 506

ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

Moscow, Russia
+7 495 974 1162

www.elcomsoft.com

ElcomSoft develops state-of-the-art computer, mobile and cloud forensics tools, provides computer forensics training. Since 1997, ElcomSoft has been providing support to businesses, law enforcement, military, and intelligence agencies. ElcomSoft tools are used by Fortune 500 corporations, military, foreign governments and all major accounting firms.

ESET

Booth 211

eset

San Diego, CA, USA
(619) 876-5474

www.eset.com

For over 30 years, ESET has been making the digital world a safer place. Through innovation and best-in-class technology, ESET secures over 100 million people around the world every day.

Evimetry

Booth 508

Evimetry
Digital forensics at wire speed

Brisbane, QLD, Australia
+61 7 3613 0082

Evimetry.com

Evimetry closes the gap between acquisition and analysis, cutting hours from forensic workflow and delivering analysis results within minutes of forensic acquisition beginning. Faster acquisition and processing cuts hours of wait time from cases, and remote agents give travel-free & reliable remote analysis of volatile memory and disk.

FINAL DATA INC.

Booth 104

FINAL DATA
Forensic Acquisition, Analysis and Data Recovery Solutions

Woodland Hills, CA, USA
(877) 612-2353

www.finaldata.com

FINALDATA Inc. specializes in digital mobile forensics solutions. With our tool, we are able to recover data from mobile devices. Our mobile forensics software is an advanced data-carving tool. We update our database at least every month to stay up to date with our User's needs.

Forensic Computers, Inc.

Booth 408

FCI Forensic Computers Incorporated

Glen Lyn, VA, USA
(540) 726-9530

www.forensiccomputers.com

Forensic Computers, Inc (FCI) has been engineering and constructing premium, custom-made forensics workstations since 1999. Designed for maximum performance and reliability, our forensic towers are the most rigorously tested and well-supported workstations on the market. We are here to help with your digital forensic needs-software, hardware, workstations, and more.

GeoTime by Uncharted Software

Booth 113

geotime

Toronto, ON, Canada
(416) 203-3003

www.geotime.com

GeoTime is a powerful visual analysis and mapping software for law enforcement, used primarily for investigative cases involving call detail records, mobile forensic data, GPS, location-tracking data, and social media data. Play back your suspect's actions, communications and key events before and after the crime.

Grayshift

Booth 606

Atlanta, GA, USA
(770) 331-4343

www.grayshift.com

Grayshift is focused on building product-based solutions for law enforcement, public safety, and national defense designed to gain lawful access to encrypted devices. Advancement in strong encryption remains a significant hurdle for law enforcement. Grayshift's GrayKey is the market leading iOS forensic access technology in use today.

Hawk Analytics

Booth 210

Bartonville, TX, USA
(706) 389-1182

www.hawkanalytics.com

Hawk Analytics was founded by a cell phone industry veteran with over a decade of experience analyzing cell phone records. CellHawk combines cell phone industry experience with an understanding of an investigators' needs resulting in an easy-to-use system for mapping, analyzing and presenting historical cell phone call detail records (CDRs).

HTCI EDAS FOX

Booth 510

Largo, FL, USA
(727) 657-1526

www.edasfox.com

For the past 14 years we have been the leading supplier of forensic computers to the Digital Forensics community. Owned and operated by a retired Law Enforcement veteran. We understand the importance of your mission and are here to assist in supplying quality products at the lowest price possible.

IACIS - The International Association of Computer Investigative Specialists

Booth 610

Leesburg, VA, USA
(407) 385-3205

www.iacis.com

Founded in 1990, IACIS is a voluntary, non-profit peer group, digital forensic training and certification organisation with almost 3000 members in over 70 countries around the world. IACIS membership, digital forensic training and certification are extremely highly regarded and are mandatory for many digital forensic units from around the world.

iPadRehab Microsoldering

Booth 206

Honeoye Falls, NY, USA
(585) 397-4174

www.ipadrehab.com

iPad Rehab Microsoldering: one-stop shop for mobile device logic board repair, training, and supplies. Restore native access to forensic data through repair.

Mail-in repair: bring dead logic boards back to life. Recover data.
- CPU/NAND swap for catastrophic damage iPhone and Samsung devices

Microsoldering training
- Practical Board Repair School
- MasterClass—CPU rework

Logicube

Booth 512

Chatsworth, CA, USA
(818) 770-8488 x123

www.logicube.com

Logicube® is a global manufacturer of digital forensic imaging and hard drive duplication solutions. Our world-class innovation delivers feature-rich solutions to government, military, education, and security organizations world-wide. Our digital forensic solutions, including our flagship Forensic Falcon®-NEO, set a new standard of excellence in forensic imaging devices.

Magnet Forensics

Booth 203

Herndon, VA, USA
(519) 342-0195

www.magnetforensics.com

Magnet Forensics is a global leader in the development of digital investigation software that acquires, analyzes and shares evidence from smartphones, computers, IoT related devices, and the cloud. Magnet Forensics has been helping examiners and investigators fight crime, protect assets, and guard national security since 2011.

MEDIACLONE

Booth 107

Reseda, CA, USA
(818) 654-6286

www.media-clone.net

MediaClone, Inc. - Develops and manufactures in the US of high performances SuperImager line of forensic imagers and complete investigation units. The units' capabilities are Extreme Fast Multi Sessions Simultaneous Imaging from many interfaces, Remote Capture from un-opened laptops, Virtual Drive Emulator, Full Forensic Analysis, Cellphone Data Extractions and Triage

mh Service

Booth 110

Kandel, RP, Germany
+49 7275 404440

www.mh-service.de/en

With more than 25 years' experience, mh SERVICE GmbH is one of today's leading providers and suppliers of products and services related to IT forensics. Europe's only forensics supplier with its own hardware development and manufacturing departments.

MOS Equipment

Booth 612

Santa Barbara, CA, USA
(805) 318-3212

www.mosequipment.com

THE WORLD'S MOST ADVANCED WIRELESS DEVICE SHIELDING — Mission Darkness is brought to you by MOS Equipment. Mission Darkness offers a comprehensive selection of radio frequency shielding solutions primarily for law enforcement and military forensic investigators, executive travel protection, and anti-hacking/anti-tracking protection.

MSAB Inc

Booth 503

Arlington, VA, USA
(703) 750-0068

www.msab.com

We enable you to unlock the full potential of mobile forensics to speed up your investigations and close more cases. We're the world leader in front line forensics, which puts easy-to-use tools in the right locations to enable fast results and actionable intelligence, with centralized control, management and reporting.

Nuix USG

Booth 502

Herndon, VA, USA
(877) 470-6849

www.nuix.com

Nuix USG understands the DNA of data at enormous scale. We pinpoint critical information government organizations need to anticipate, detect, and act on risk, compliance, and security threats. Our platform identifies hidden connections between people, objects, locations, and events—providing real-time clarity, control, and efficiency to uncover key facts.

Open Text, Inc. | EnCase

Booth 410

Waterloo, ON, Canada
(262) 832-6843

www.guid.com

OpenText™ is the leader in Enterprise Information Management (EIM). Our OpenText™ EnCase™ and Tableau hardware products are the gold standard for digital forensic investigations. Together, they provide solutions for the entire case lifecycle – from triage to reporting.

OSForensics

Booth 109

Redwood City, CA, USA
(417) 455-3589

www.OSForensics.com

OSForensics by PassMark Software is an incredibly powerful and ultra-fast computer forensic and live-analysis software. OSForensics offers users the first straightforward, affordable solution, designed to handle all elements of today's digital investigations, both out in the field, and in the lab. OSForensics…Digital investigation for a new era.

Oxygen Forensics

Booth 403

Alexandria, VA, USA
(877) 969-9436

www.oxygen-forensic.com

Oxygen Forensics was founded as a PC-to-Mobile Communication software company. This experience has allowed our team to become unmatched in understanding mobile device communication protocols. With this knowledge, we have built innovative techniques into our products allowing our users to access critical information from mobile devices, clouds and drones.

Passware

Booth 409

Mountain View, CA, USA
(650) 472-3716 x105

www.passware.com

Passware is the world leader in password recovery, decryption and encrypted electronic evidence discovery software for Federal and State agencies, Fortune 500 corporations, law enforcement, corporations and private investigators. Our flagship product, Passware Kit Forensic, supports decryption for 280+ file types, encrypted hard drives, mobile devices and cloud data acquisition.

PenLink

Booth 507

Lincoln, NE, USA
(402) 421-8857

www.penlink.com

PenLink provides communications surveillance collection systems to law enforcement agencies. Our solutions ingest historical data, or live-collect from service providers, to normalize native file formats or delivery standards for easy analysis. PenLink is headquartered in Lincoln, Nebraska, with offices in Boulder, Colorado, and Washington D.C. For more information, visit www.penlink.com

RUSOLUT

Booth 108

Warsaw, Poland
+48 222 562 272

www.rusolut.com

We are glad to present unique and the only groundbreaking solution for data extraction and recovery from eMMC chips through NAND interface - eMMC Nand Reconstructor! If your solution can not do the same - visit booth 108!

SciEngines

Booth 406

Kiel, SH, Germany
+49 431 9086 2008

www.sciengines.com

SciEngines enables Digital Forensics experts to recover passwords and encrypted evidence faster than ever. This is what we truly excel in like nobody else. Our special-purpose high-performance systems are also highly economical, outstandingly energy-efficient and scalable beyond measure. Take us to the test at booth 406.

Searchlight Security Darknet Intelligence

Booth 511

Portsmouth, Hampshire, United Kingdom
+44 2380 981303

www.slcyber.io

Searchlight Security Ltd is a world leading darknet intelligence and Forensics Company serving law enforcement, private investigators and cyber security firms. Our tools set allow investigation, due diligence and live alerting all structure in a case management system.

SentinelOne

Booth 604

Mountain View, CA, USA
(408) 205-0384

www.sentinelone.com

SentinelOne delivers autonomous endpoint protection that successfully prevents, detects and responds to attacks across all major vectors. SentinelOne applies AI to automatically eliminate threats in real time and provides full visibility across networks directly from the endpoint. Visit sentinelone.com or follow us at @SentinelOne, on LinkedIn or Facebook.

South Carolina Electronic Crime Task Force

Booth 509

Columbia, SC, USA
(803) 896-7901

www.sled.sc.gov

The South Carolina Electronic Crimes Task Force is a strategic alliance of law enforcement, academia and corporate sector stakeholders, dedicated to proactively disrupting, deterring and investigating cyber related attacks on South Carolina and the Nation's critical infrastructure sectors.

Sumuri LLC

Booth 112

Wyoming, DE, USA
(302) 570-0015

www.sumuri.com

SUMURI is a leading worldwide provider of solutions for digital evidence and computer forensic training, hardware, software and services. SUMURI is also the developer of the industry standard PALADIN Forensic Suite, RECON, CARBON Virtual Forensic Suite and TALINO Forensic Workstations.

Susteen, Inc.

Booth 311

Irvine, CA, USA
(949) 789-8208

www.susteen.com

Susteen, Inc. is a world leader in mobile forensics and data communications. Our new cutting-edge DataPilot 10 Field Triage Device makes it easier than ever to acquire data in real-time. Headquartered in the United States, we are proud to be a driving force in keeping our communities safe.

T3K-Forensics

Booth 317

Vienna, Austria
+43 699 132 375 43

www.t3k-forensics.com/en

T3K-Forensics brings artificial intelligence to mobile forensics, developing unique software solutions for automated analysis of smartphone data extractions, to help simplify and speed up mobile forensic investigations.

Teel Technologies

Booth 517

Norwalk, CT, USA
(203) 855-5387

www.teeltech.com

Teel Technologies provides the best tools, training and services for professionals tasked with investigating mobile devices. We focus on the total lab establishment, training in all skill levels, and expert servies. Our unyielding credo of integrity and quality ensures customers receive the best service and support in the industry.

Tri-Tech Forensics

Booth 306

Leland, NC, USA
(910) 208-9961

www.tritechdf.com

TRITECHFORENSICS' DF Division focuses on efficiency at an affordable price. Knowing you must be supplied with exceptional tools, we concentrate on meeting the specific needs of your agency through our customized equipment and faraday products. We also offer many items through GSA schedules, providing you with a simple purchasing experience.

Truxton Forensics

Booth 208

Herndon, VA, USA
(571) 730-0020

www.truxtonforensics.com

Truxton is a multi-user forensic platform with distributed processing, automated analysis, and cross-case/media correlation capabilities. Designed for multi-agency, enterprise, and field applications, it provides customizable, automatic tagging of specific data types, and an industry-first "Pocket Litter" feature that allows correlation between physical items and digital data. Visit www.truxtonforensics.com.

Ultra Tec Mfg., Inc.

Booth 209

Santa Ana, CA, USA
(703) 350-5834

www.ultratecusa.com/chip-digital-forensics

ULTRA TEC has developed a range of "Cold Chip-Off" digital forensics tools (precision milling, sawing and flat grinding) that keep process temperatures low allowing users to prepare NAND flash devices with consistent high yields. Chip-Off is an important technique for professionals who need to access data from mobile devices.

Vound Software

Booth 602

Phoenix, AZ, USA
(888) 291-7201

www.vound-software.com

Vound is a leading global vendor of technology used for end-to-end forensics search and eDiscovery. Intella is a 1 stop shop for digital investigators enabling end users to index cell phone, email, disk images, load files and more at market leading speed & processing power-at the industry's best value.

Whooster

Booth 212

YOUR PARTNER FOR INVESTIGATIVE DATA

Buda, TX, USA
(512) 419-4210

www.whooster.com

Whooster delivers investigative data solution tools to law enforcement, government agency and private sector clients who need real-time delivery of accurate data on the location, phones and background of individuals and businesses. Through SMS / Text Messaging, Web Based, Batch, Direct Connect and Integrated DaaS Solutions Whooster Data Fusion technology delivers fresh, reliable data needed for enforcement, regulatory, and private concerns.

ZETX

Booth 411

Chandler, AZ, USA
(844) 367-9389

www.zetx.com

ZetX is the leader of cloud based, forensic mapping and analysis tools for Law Enforcement. Using a CJIS compliant platform, radio frequency horizontal planes, astounding real time applications, and unrivaled training, ZetX resources are heralded for their ease of use and unparalleled accuracy. Train, demo or ask questions at www.zetx.com.

Thank You to Our 2019 Advisory Board!

Robert Boggs – Corporal - Digital Forensics Analyst, West Virginia Police

Jeffrey H. Carrington – Senior Cyber Security SME, HP/Perspecta

Julius Clark – Cybersecurity Instructor, Mission Critical Institute

Stacey Coleman – Program Coordinator, Aiken County - Office of the Solicitor - 2nd Judicial Circuit

Phillip Comer – Information Security Consultant, Engineer, Architect, Phoenix Data Security

Byron S. Cousin Sr. – Tactical Exploitation Instructor, U.S. Army Retired

Julie Fetcho – Regulatory Affairs Officer, TIAA-CREF

Abdul Hassan – CEO, International Counter Terrorism Forensics Foundation

Bryan Hill – Technology Architect, Booz Allen Hamilton

Alfred Johnson – CEO/Chief Investigator, JLA Investigations & Security LLC

Jim Keegan – Director, Information Security, CISSP, Q/EH, Essent Guaranty

Dennis W. Kuntz – Manager, Vulnerability Management, Amazon

Carl Letourneau – Digital Forensics Investigator, Canada Border Services Agency

Giovanni Masucci – Sr. Digital Forensic Examiner, North Carolina State Licensed Counterintelligence Professional and President of National Digital Forensics, Inc.

Erik J. Modisett – Cyber Investigations Technical Manager, U.S. Customs & Border Protection, Air and Marine Operations

Robert Reynolds – Chief Information Security Officer, Town of Chapel Hill

Sue Rusher – IT Auditor, BlueCross BlueShield of SC

Alan Tumey – Senior Security Analyst, Global Security Operations, CISSP, CISM, CISA, VF Corporation

David Vargas – VATG, Inc., Professor of Networking and Cybersecurity, George Washington University and Montgomery College

Helen Weathers – Crime Scene Supervisor, South Fulton County Police Department

Karla Weinbrenner – Instructor - Digital Forensics and Cyber Security, ACE, Cumberland County Guardian ad Litem, Methodist University

Tim Yeager – Senior Computer Engineer, Air Force Research Laboratory

Thank You to Our 2019 Industry Supporters!

CYBER·SC

DIGITAL FORENSIC COMMUNITY

ENTERPRISE SECURITY

FORENSIC FOCUS
FORENSICFOCUS.COM

govCIO OUTLOOK

HTCIA

INFRAGARD SOUTH CAROLINA MEMBERS ALLIANCE

ISACA
Trust in, and value from, information systems
SC Midlands Chapter

MYTECHMAG

NW3C

WOMEN IN eDISCOVERY
WOMEN EMPOWERING WOMEN

Techno Security & Digital Forensics Conference






Save the Date!

The goal for Techno Security & Digital Forensics Conference is to deliver a unique conference experience that blends together the digital forensics and cybersecurity industries for collaboration between government and private sectors. These events will continue to be a valuable resource for IT security professionals granting an opportunity for discussion and information, while bringing together the industry's leading decision makers with the aim to raise international awareness of developments, teaching, responsibilities and ethics in the field of cybersecurity and digital forensics.

San Antonio, TX | **September 30 - October 2, 2019**
Hyatt Regency Hill Country Resort and Spa

San Diego, CA | **March 9-11, 2020**
Hilton La Jolla Torrey Pines

Myrtle Beach, SC | **May 31 - June 3, 2020**
Marriott Resort at Grande Dunes

www.TechnoSecurity.us

COMEXPOSIUM
www.comexposium.com

Notes

HOST SPONSORS

Cellebrite — Digital intelligence for a safer world

MAGNET FORENSICS

DIAMOND SPONSORS

Belkasoft — forensics made easier

OXYGEN FORENSICS

PLATINUM SPONSORS

ACCESSDATA

CRU

DATAPILOT

GRAYSHIFT

MSAB

nuix

opentext™

T3K-Forensics

TEELtechnologies

ZETX — ADVANCING JUSTICE

GOLD SPONSORS

ACELab®

ADF

ARGENT

BlackBag TECHNOLOGIES

COBWEBS TECHNOLOGIES

DeSales University

DMEforensics — Focused Digital & Multimedia Evidence Solutions

EDEC

ELCOMSOFT — DESKTOP, MOBILE & CLOUD FORENSICS

eset

Evimetry — Digital forensics at wire speed

FCI — Forensic Computers Incorporated

geotime

HAWK ANALYTICS

HTCI EDAS FOX LLC

IACIS — The International Association of Computer Investigative Specialists

iPadRehab MICROSOLDERING

Logicube®

MISSION DARKNESS — Made By MOS Equipment — www.mosequipment.com

Passware

PENLINK

SciEngines — massively parallel computing

SEARCHLIGHT Security

SentinelOne™

TRITECH DIGITAL FORENSICS — identify. collect. preserve.

TRUXTON

ULTRATEC MANUFACTURING, INC.

Vound Intella

WHOOSTER.COM — YOUR PARTNER FOR INVESTIGATIVE DATA

SILVER SPONSORS

ACETECH PARTNERS

Atola TECHNOLOGY

AVAIL Forensics

BERLA

CYAN FORENSICS

Digital Intelligence — mastering the science of digital forensics

FINAL DATA — Forensic Acquisition, Analysis and Data Recovery Solutions

MediaClone

mh SERVICE GmbH

OSForensics by PassMark Software

ruSolut

SUMURI


Cellebrite
Digital Intelligence
for a safer world
Access digital data faster
Realize hidden connections
Act on the evidence
STOP BY BOOTH #303
www.cellebrite.com