Techno Security & Digital Forensics Conference

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

2020 Event Guide

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

www.TechnoSecurity.us

COMEXPOSIUM
www.comexposium.com

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.

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

Denver, CO | **October 26 - 28, 2020**
Hilton Denver City Center

San Diego, CA | **Spring 2021**
Announcement Coming Soon

www.TechnoSecurity.us

COMEXPOSIUM
www.comexposium.com

Techno Security & Digital Forensics Conference

Welcome to the second edition of the California 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 2020 program will feature 75 sessions led by 69 industry experts plus 35 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 2020 Event Management Team

Table of Contents

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 **#TechnoSecurityCA** 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

Monday, March 9

12:00pm	–	1:00pm	Sessions
1:15pm	–	2:15pm	Sessions
2:00pm	–	6:00pm	Exhibit Hall Open
2:15pm	–	2:45pm	Networking Break in Exhibit Hall
2:45pm	–	3:45pm	Sessions
4:00pm	–	5:00pm	Sessions
5:00pm	–	6:00pm	Show Floor Happy Hour Reception

Tuesday, March 10

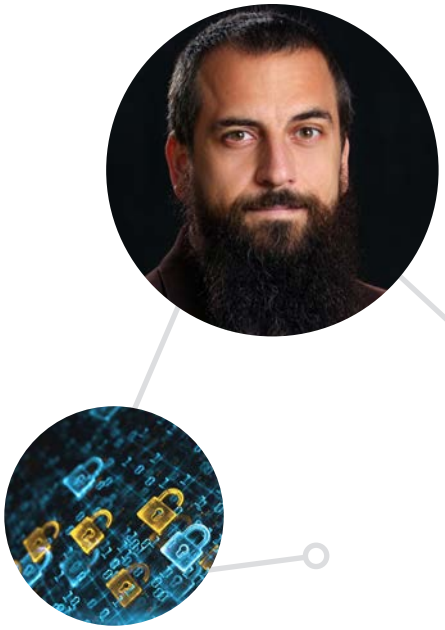
7:30am	–	8:00am	Morning Coffee
8:00am	–	9:00am	Keynote
9:00am	–	9:30am	Networking Break
9:30am	–	10:30am	Sessions
10:45am	–	11:45am	Sessions
11:00am	–	4:30pm	Exhibit Hall Open
11:45am	–	1:30pm	Dedicated Exhibit Hall Hours
12:00pm	–	1:00pm	Lunch
1:30pm	–	2:30pm	Sessions
2:30pm	–	3:15pm	Networking Break in Exhibit Hall
3:15pm	–	4:15pm	Sessions
4:30pm	–	5:30pm	Sessions
5:30pm	–	6:30pm	Reception

Wednesday, March 11

7:30am	–	8:00am	Morning Coffee
8:00am	–	9:00am	Early Riser Session
9:15am	–	10:15am	Sessions
10:30am	–	11:30am	Sessions
11:00am	–	3:30pm	Exhibit Hall Open
11:30am	–	1:30pm	Dedicated Exhibit Hall Hours
12:00pm	–	1:00pm	Lunch
1:30pm	–	2:30pm	Sessions
2:30pm	–	3:15pm	Networking Break in Exhibit Hall
3:15pm	–	4:15pm	Sessions

Roman V. Yampolskiy, Ph.D.

Futurist, Author, Professor



Artificial Intelligence and the Future of Cybersecurity

Tuesday, March 10 | 8:00am – 9:00am

Dr. Roman V. Yampolskiy is a Tenured Associate Professor in the department of Computer Engineering and Computer Science at the Speed School of Engineering, University of Louisville. During his teaching career, he has received multiple recognitions that include (but are not limited to): Distinguished Teaching Professor, Professor of the Year, Leader in Engineering Education, Top 4 Faculty, and Outstanding Early Career in Education award. He is the founder and director of the Cyber Security Lab. In addition, he has authored many books, including his latest publication, *Artificial Superintelligence: A Futuristic Approach*.

Refer to page 12 for full session description

The Dark Web & Crypto Currency Investigations

Wednesday, March 11 | 8:00am – 9:00am

Under the cloak of darkness, criminals are using tools for privacy and anonymity to commit a wide range of crimes on the Dark Web using Crypto Currency. During this session, attendees will learn some investigative tips and tricks to combat this new way of committing old crimes.

Presented by:

Joe Saar – Detective, Costa Mesa Police Department

Joe is a Detective in the Costa Mesa Police Department's Special Investigations Unit. His primary assignments include investigations in human trafficking, narcotics, financial, and violent crimes. Prior to joining the Costa Mesa Police, Joe served as an Infantry Officer in the United States Marine Corps. Joe holds a Bachelor's Degree in Government and Politics from St. John's University in Queens, New York, and a Master's Degree in Business (MBV) from the Marshall School of Business at the University of Southern California.

Rahul Gupta – Senior Trial Deputy, Orange County District Attorney's Office

Mr. Gupta is a Senior Trial Deputy for the Orange County District Attorney's Office. He specializes in prosecuting cyber-crime in the Major Fraud unit. Mr. Gupta has a background in technology and frequently teaches attorneys and law enforcement officers throughout California on digital evidence, social media, dark web and crypto currency related topics.

Refer to page 20 for full session description

Monday, March 9

The 2020 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** **Sponsor Demo**

12:00pm – 1:00pm

Grande D

Collection, Preservation, and Analysis of Digital Video Evidence
Motti Gabler, Forensic Expert, National Center for Audio and Video Forensics

This session will educate investigators, law enforcement, and prosecutors on proper methods for the collection, preservation, and analysis of digital video evidence. With this knowledge, police and prosecutors will be better equipped to enhance and present video evidence in court. The session will discuss relevant factors in understanding video evidence such as resolution, frame rate, and video compression as well as how these factors may affect the case.

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

Grande E

The Practicality of Cyber Resilience
Ronald O'Neal, Senior Practitioner, Treuvizion Consulting Corp

As cyber risk continues to diversify and become more strategic, Cyber Security focus increases and evolves. Melting in a level of Cyber Resilience becomes more paramount. Establishing a risk driven focus around business operations, with a holistic resilience framework is becoming more of a magic trick than a strategic plan. This session will discuss: Trends in Cyber Resilience; Understanding the role of resilience in Cyber Strategies; and the Future of Cyber Resilience.

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

Scripps I

Use Common Passwords to Access Mobile Devices
Jeremy Kirby, Director of Sales, Susteen, Inc.

Many phones are locked and inaccessible to lab personnel. Our engineers have used algorithms and gathered the most commonly used pincodes/passcodes for different forensic cases. Learn the most commonly used pincodes/passcodes for sex offenders, drug dealers and the average person. Attendees will be provide the list to better help keep your communities safe. Save time and money by learning how to effectively use these codes in the field or back in the lab.

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

Scripps II

A Risk Management Conversation on the Shift in Regulatory Landscape and What Financial Services Can Teach Technology Companies
Melike Etem, Global Security Office, GRC, Symantec Corporation

Technology companies, long left largely unregulated, face a brave new world. Given growing concerns over data protection and cybersecurity, public scrutiny is increasing. As good corporate citizens, how can technology companies reshape their journey and get ahead of these new developments? During this session, attendees will learn about the following concepts at a high level: Enterprise Risk Management; Governance, Risk and Compliance; Enterprise Risk Management Governance Framework; Architecting Enterprise Risk Management; Risk Appetite; and Risk Reporting.

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

12:00pm – 1:00pm (continued)

Canyon

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: LEAP: Law Enforcement Analytic Platform, for high-speed triaging and analysis of forensics images. Also applicable for border control, particularly anti-trafficking and counterterrorism.

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

Shore

Today's Digital Investigations using Artificial Intelligence
Rene Novoa, Account Executive, Oxygen Forensics

Have a case that contains 100,000 images and you are literally looking for the needle in the haystack that happens to be a red needle? This is what today's digital investigations have come to, often an unreasonable expectation. It is not uncommon for an investigator to have to look through media that has been extracted from multiple sources like mobile devices, cloud services, IoT devices, and UAS for an image of importance. More times than not the investigation cannot be completed simply due to time constraints imposed by the type of investigation. In the case of exigent circumstances this time is not available, and taking this time could lead to a grave outcome. Incorporating the use of artificial intelligence to "fine tune" the searching of the data will often deliver results that most investigators would not believe. By using AI to train software in today's investigations can not only save time, but save lives.

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

Monday, March 9 (continued)

The 2020 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** **Sponsor Demo**

1:15pm – 2:15pm

Grande D

Finding the Best Starting Point for Insider Threats and Other Workplace Investigations
Trey Amick, Forensics 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. Join the presenter for a 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. This session will 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; and Prove intent by visualizing relationships between files and actions.

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

Grande E

Protecting your Data and System from Ransomware Saves Money and is Good for Business
Don Malloy, Chairman, Initiative for Open Authentication

The number of ransomware attacks has increased over 700% annually. The current approach of the attacker involves the ability of going after the backup of the data. There is a strong need to protect against the backup becoming the target. During this session, the presenter will discuss with the audience: Why backups are not secure; Using multi factor authentication, the user will gain additional level into the ability to have secure authentication; and How the users data will be protected from the hackers changing and encrypting the data.

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

Scripps I

FBI Next Generation Identification
Michael Lohmann, Supervisory Biometric Images Examiner, FBI

The session will include a high-level overview of the FBI Next Generation Identification (NGI) System person-centric biometric modalities to include ten print, latent print, facial recognition and other criminal history information services offered by the FBI.

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

Scripps II

Where Should I start with the NIST Cyber Security Framework?
John Riley, CEO, Omnistruct, Inc.

There are a number of frameworks available to base your organizations' cybersecurity, but the latest of these has been provided to us by the US Government. There will be something for everyone to learn at this session whether you are just starting your journey towards cyber-compliance or if you are well on your way. Attendees will learn: Why is it important to use a framework?; Three different levels of NIST CSF; and Where to begin for their organization?

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

1:15pm – 2:15pm (continued)

Canyon

Tips and Tricks with Blacklight 2019R3
Stephanie Thompson, Solutions Engineer, BlackBag Technologies

Blacklight 2019R3 brought some new and improved functionality. This demo will share some of the new features to help you in your investigations including: New Processing options to help triage data; Parsing of Apple Unified Logs; New Windows Artifacts Parsed in Actionable Intel; Passware Integration to decrypt images of devices with full disk encryption; Redesign of File Filters enabling the creation of complex file filters; Additional support for processing Cellebrite extractions; Support added to process macOS 10.15 Time Capsule backups; and more.

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

Shore

Cellphone Data: Investigation, Analysis and Presenting Your Case to Others
Adeel Khamisa, Director, Law Enforcement Industry - GeoTime, UnCharted Software, Inc.

This session will provide an overview of more up-to-date methods of handling cellphone records, beyond Microsoft Excel. It will address common mistakes analysts make in requesting, formatting and presenting cellphone data from call detail records (CDRs) and mobile forensic extractions. The session will also focus on easily identifying a suspect's pattern of life and how to present that in court. Attendees will have the opportunity for a follow-up online hands-on training session for practical application.

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

2:45pm – 3:45pm

Grande D

From 0 to Accreditation
Mark Spooner, Director, Dixie State University

What does it take to bring a digital forensic lab into full accreditation status? The attendees will learn from the director of a digital forensic lab that is currently undertaking international accreditation what goes into the planning process, the execution process, and the reasoning behind the decision making process to obtain full lab accreditation. Starting from ground zero, the Digital Forensics Crime Lab (DFCL) at Dixie State University in Southern Utah began FY20 by devoting resources, monetary and personnel, to begin the process in order to obtain full lab accreditation through the American Association for Laboratory Accreditation (A2LA). Future trends will also be discussed regarding the potential for mandatory lab accreditation along with the process of determining future ROI and other growth opportunities that present themselves when running an accredited digital forensic lab.

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

Scripps I

Catalina: A Voyage Through Apple's New Artifacts
Derrick Donnelly, Chief Scientist, BlackBag Technologies

Hear from the Apple experts how Catalina's new organization of system verses user files may change investigative techniques. In addition, this session will cover what users can expect to extract from unified logs and new Spotlight results.

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

Scripps II

Proving a Negative: Case Studies Illustrating Methods to Safeguard the Organization from Something That Didn't Happen
D. Kall Loper, Director, National Lead for Incident Response, Protiviti
Mike Lefebvre, Associate Director, National Lab Director, Protiviti

Organizations face growing scrutiny and uncertainty over breach and cyber incident response. Regulators and public perception demand that corporations disclose before even understanding the issue. This session will share three recent responses, provided as case studies to illustrate both technical and strategic innovations required to protect the good name of good organizations.

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

Monday, March 9 (continued)

The 2020 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** **Sponsor Demo**

2:45pm – 3:45pm (continued)

Canyon

Identification, Acquisition and Analysis of Vehicle Systems using the iVe Ecosystem
Ben LeMere, CEO, Berla Corporation

Vehicles hold a vast amount of data that can be used to uncover critical information during an investigation and help determine what happened, where it occurred, and who was involved. The iVe Ecosystem is a collection of tools to acquire data found within vehicle systems. This session will feature a walk-through demonstration of a vehicle system forensic acquisition, best practices when examining a vehicle and the importance of the vehicle forensics process when working with multi-disciplined team.

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

Shore

Android App Analysis
Tarah Melton, Forensics Consultant, Magnet Forensics

With the millions of applications available to users on Android devices, it becomes impossible for commercial tools to be able to parse and support them all. This makes it critical to understand how applications are stored on these devices and where to find that important data that could be vital to your case. Join us as we walk through the basics of Android applications, with additional detail given to digging into SQLite database files where much of that application data is stored. See how enhanced features found in Magnet AXIOM, such as the Dynamic App Finder and our built-in SQLite Viewer, can help you review and report on the application data in your case quickly and efficiently. Then with the free tool, the Magnet App Simulator, see how to view and interact with Android application data in a virtual environment.

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

2:45pm – 5:00pm

Grande E

In Real Life IR made Simple: creating Speed, Synergy & Accuracy to your IR workflow
Gregg Braunton, Sr. Cyber Solutions Architect – Healthcare Digital Health Services, Leidos

In this session, attendees will learn about the "Storyboard" Incident Response Methodology. A simple, effective, repeatable, and extremely visual methodology, participants' eyes and mind will pop with that "ah-ha" moment that will instantly make them converts to storyboarding and ask themselves, "Why didn't I think of that?". The presenter will share high level objectives of how attendees will learn the practical application of storyboarding to effectively support all phases of the incident response process.

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

4:00pm – 5:00pm

Grande D

Cloud Data Methods for Capture
Amber Schroader, CEO, Paraben Corporation

As more and more data move to the cloud understanding some of the ins and outs of how and what you can capture is important for any examiner. This session will review how the cloud is storing data, when it can be captured, and methods and the data that is captured. Both mobile capture and options for desktop cloud data will be discussed.

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

4:00pm – 5:00pm (continued)

Scripps I

Cyber Incident Response — Preparing for the Inevitable!
Matt Meade, Partner, Eckert Seamans Cherin & Mellott, LLC
Serge Jorgensen, President, Sylint

Cyber incidents are often the result of an escalating series of technical and non-technical failures which include lack of preparation, lack of adequate employee training designed to increase awareness of risky behavior and incomplete or non-existent evaluations and protections involving vendors and other third parties who receive valuable data from the organization. During this session, attendees will work through a series of hypothetical security incidents involving data theft, ransomware and data exposure and will learn: Cyber best practices; the Importance of a proactive approach to cyber security; and State and Federal law issues associated with responding and reacting to a security incident.

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

Scripps II

Using Drone Forensics in Criminal Investigations
Erik Modisett, Supervisory Agent, U.S. Customs and Border Protection

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

This session will discuss how a sUAS intercepted along the border near San Ysidro became the first Federal conviction of a narcotics smuggler using the unmanned delivery platform. The session will focus on preservation of the evidence to actual extraction and analysis of the aircraft's flight logs. The Case Agent will discuss how he integrated this unique set of data into the prosecution package and how it affected his investigative methods. The conclusion will cover how this case has since evolved CBP's sUAS data forensic capabilities and how CBP assists agencies around the world grow and develop their own drone forensic capabilities.

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

Canyon

Hands-On with DATAPILOT 10: The Acquisition Device You Need
Jeremy Kirby, Director of Sales, Susteen, Inc.

FASTER, FRIENDLIER, MORE AFFORDABLE: Be the first to see our new cutting-edge technology for acquiring only the evidence you need, instantly from digital devices. This hands-on demo will change your perception about how, when and where to acquire your digital evidence and triage instantly. See what thousands of agencies have deployed in the field and in their labs. Be the first to see our new Data Acquisition Method.

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

Shore

Tableau Forensic Imager (TX1): Next-Generation Features for Today's DFIR Imaging Challenges
Jeff Hedlesky, Partner Success Manager, OpenText, Inc.

See the new Tableau Forensic Imager (TX1) feature suite demonstrated, which spans advanced logical imaging, a remote Web interface, including forensic triage / file collection, user account management, enhanced drive detail reporting, enhanced PCIe device handling (clone, wipe, format), AMA recovery, Imaging process Pause & Resume, OPAL drive decryption, a preview of our new TX1 API for device automation and integration into forensic lab workflow, and much, much more.

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

Tuesday, March 10

The 2020 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** **Sponsor Demo**

8:00am – 9:00am

Grande D/E **Keynote: Artificial Intelligence and the Future of Cybersecurity**
Roman Yampolskiy, Futurist, Author, Professor, University of Louisville

The rise of AI-enabled cyberattacks is expected to cause an explosion of network penetrations, personal data thefts, and an epidemic-level spread of intelligent computer viruses as well as fake forensic evidence. Ironically, our best hope to defend against AI-enabled hacking is by using AI. Will AI enhance cybersecurity or make it more difficult to create robust defenses for cyberinfrastructure? During this keynote presentation, Dr. Roman Yampolskiy will discuss the paradox that AI will bring for cybersecurity and how cybersecurity experts can prepare to address impact from AI.

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

9:30am – 10:30am

Grande D **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. In this session we will also investigate APFS Operating System artifacts and files such as: KnowledgeC.db, FSEvents, Volume Mount Points, Quarantined Files, and bash history, providing context on how these artifacts will help connect the dots in your investigations.

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

Grande E **What Surveillance Capitalism Means For You: Cybersecurity & Privacy Threats Posed by Smartphones, Tablet PCs and Connected Products**
Rex Lee, Cybersecurity and Privacy Advisor/Tech Journalist, My Smart Pivacy/BLACKOPS Partners

Attendees will learn cybersecurity, privacy, civil liberty and safety threats associated with surveillance and data mining business practices employed by tech and telecom giants such as Google, Apple, Microsoft, Amazon, Facebook, Tencent (China), Baidu (China), Prisma Labs (Russia), and so on. They will also learn about intrusive apps that support smartphones, tablet PCs, connected products, and PCs supported by the android OS, Apple iOS, and Microsoft Windows OS.

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

Scripps I **Peak Inside Windows Memory: A Toolbox Approach**
Lynita Hinsch, Digital Forensics Investigator, Allstate Insurance Corporation

This session will share the fundamentals of memory analysis using industry proven open source software tools such as Volatility and BulkExtractor. Learn how to download, install, and configure the tools on your forensic workstation, run essential commands and plugins to conduct memory examinations, and interpret the output and results. Compare the command line output of the open source tools with additional tools you may already have in your toolbox to see how to streamline and automate your memory examinations. If your lab isn't conducting memory analysis, this is how to start!

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

9:30am – 10:30am (continued)

Scripps II

2020 Vision: Preparing for the California Consumer Privacy Act
Joseph Pochron, Senior Manager, Forensic & Integrity Services, Privacy & Cyber Response, Ernst & Young LLP
Justine Phillips, Cyber & Employment Attorney, Sheppard Mullin
Ruth Hauswirth, Special Counsel Information Retention Counseling & Litigation and E-Discovery Services, Cooley LLP

Although California's Consumer Privacy Act (CCPA) was intended to govern digital giants like Facebook, it will also impact small and medium-sized businesses. Effective Jan. 1, 2020, the sweeping digital privacy law gives consumers new rights over their personal information—and comes with financial risk related to non-compliance for the companies that hold it. During this panel discussion, attendees will learn: Whether CCPA applies to your organization; What is "reasonable security" under CCPA and how to demonstrate it; Why CCPA is a catalyst for holistic information governance and What steps to take now to prepare for the new regulations.

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

Canyon

Bridging Accessibility Between Mobile Phone and Vehicle Data
Ben LeMere, CEO and Co-Founder, Berla Corporation
Derrick Donnelly, Chief Scientist, BlackBag Technologies

With the recent partnership between BlackBag and Berla, investigators now have the ability to export a file to a proprietary format that can be opened in BlackLight, BlackBag's flagship forensic tool for analyzing Windows, Android, iOS, and macOS devices. With this functionality, agencies can import data acquired by iVe, from a vehicle's infotainment system into a BlackLight case and view it alongside other device data. This session will give investigators the tools to take full advantage of the recent integration of iVe and BlackLight.

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

Tuesday, March 10 (continued)

The 2020 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** **Sponsor Demo**

9:30am – 10:30am (continued)

Shore

Aggregating Data from Disparate Data Sources
Dave Ryberg, Director of Truxton Sales, Truxton Forensics

The advent of new, cost-effective acquisition tools like Datapliot, ADF, E3, and other products has made digital forensics easier and more affordable than ever before. Come see how your team can simultaneously review, correlate, and analyze multiple investigations from any source using Truxton's automated tagging, artifact discovery, and reporting features.

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

10:45am – 11:45am

Grande D

Using Open Source Tools in an Attempt to Defeat Encryption
Felipe Chee, District Attorney Investigator, San Diego County District Attorney's Office

Trying to defeat encryption with a word list increases your odds of bypassing encrypted file(s). An overview of various tools will be presented that are used in the acquisition of data sets and the creation of a wordlist. With a generated wordlist, it can be ingested into open source password cracking software commonly used by pen testers.

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

Grande E

Performing a Professional Web Application Penetration Test
Scott Miller, Security Consultant, Synopsys

This session will describe how to approach a professional web application penetration test, including where in the application to start, what kinds of tests to do, and how to know when to stop. The presenter will share several tools and processes that helped focus efforts on certain parts of the application without losing significant coverage on the rest of it. By the end of the session, attendees will: Have a good foundation for becoming a penetration tester; an Understanding why applications fail; and How to find the issues about which your clients care most.

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

Scripps I

Using Artificial Intelligence to Augment Threat Hunting and Incident Response
David Petty, Director, OpenText
Kevin Golas, Director of World Wide Security Services, OpenText

There is rarely a shortage of log files and other forms of evidence when threat hunting or conducting an IR investigation. Quite often there is more data than can be effectively reviewed. This session will discuss various application of Artificial Intelligence to the conduct of Incident response investigations and threat hunting engagements. The session will explore how the tools are used and on what types of data they are used with and share both opensource solutions and proprietary solutions. Attendees will leave with an understanding of how Artificial Intelligence techniques can be applied.

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

10:45am – 11:45am (continued)

Scripps II

Advanced Image Analysis in Digital Forensics
Justin Tolman, Director of Training, AccessData

In recent years, digital forensics has undergone a major shift from primarily analyzing desktop computers to now investigating smartphones, tablets and other portable digital devices in almost every investigation. As the technology evolves to include more sophisticated cameras, sound recording capabilities, Siri and more, so too must the processes and tools used to analyze data collected from these devices in a forensic investigation. This session will take take a deeper dive into advanced image analysis to help attendees understand how location data is stored within media files, and how tools like Forensic Toolkit (FTK) and Python can help investigators glean key insights and evidence from that image data during an investigation.

Target Level: Advanced
Target Audience: Law Enforcement/Police

Canyon

Hands-On with DATAPILOT 10: The Acquisition Device You Need
Jeremy Kirby, Director of Sales, Susteen, Inc.

FASTER, FRIENDLIER, MORE AFFORDABLE: Be the first to see our new cutting-edge technology for acquiring only the evidence you need, instantly from digital devices. This hands-on demo will change your perception about how, when and where to acquire your digital evidence and triage instantly. See what thousands of agencies have deployed in the field and in their labs. Be the first to see our new Data Acquisition Method.

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

Shore

Addressing the Serious Threat of Cybercrime with Magnet AXIOM Cyber
Trey Amick, Forensics Consultant, Magnet Forensics
Tarah Melton, Forensics Consultant, Magnet Forensics

Cybercrime provides its own unique challenges. Every case of fraud, workplace harassment, insider threats, identity theft, data exfiltration, IP theft, network intrusions, malware and ransomware attacks have the potential to devastate not only individuals, but corporations of all sizes. In fact, in 2015, cybercrime cost the world over $3 trillion and if current trends continue, it's predicted that by 2021 the cost of cybercrime will be in excess of $6 trillion. When cybercrime occurs, it's critical to understand the extent of what was done, how it happened, and who did it. The presenter will share a new solution that helps digital forensics professionals acquire and examine evidence from computer, mobile, and cloud sources and is purpose-built to address the unique challenges presented by cybercrime. The presenter will demonstrate the power of AXIOM Cyber including: Creation and deployment of a remote acquisition agent that can connect to and collect evidence from target endpoints; Collection of evidence from Amazon S3 buckets; and the Use of Admin credentials to acquire evidence from a user's account in Enterprise deployments of Google, Microsoft, and Box as well as Slack.

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

1:30pm – 2:30pm

Grande D

Iran, GeoPolitics and Cyber War, Past, Present and Future: A Look at the Tools and Tactics of the Nation State Adversary
Steven Bolt, Manager of Global Security Operations and Engineering, Bechtel

This session will explore the past and present for the Iranian cyber threat, from initial connection to the Internet to an up and coming operational cyber powerhouse. Topics covered will include an analysis of the political environment, loyalties of the threat groups, targets, tactics, methods and indicators. As one of the leading targets of US Cyber operations over the last 40 years, Iran has evolved and is now quite adept at launching attacks of their own, targeting internal social reformers to foreign public and private organizations. Attendees will leave with a better understanding of the Iranian threat, threat intelligence resources, as well as indicators of compromise and attack.

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

Tuesday, March 10 (continued)

The 2020 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** **Sponsor Demo**

1:30pm – 2:30pm (continued)

Grande E

What's Running on My Network, Who Is Running It and What Are They Doing With It!
James T. Mandelbaum, Sr. Security Engineer, Gigamon

With an ever-expanding network perimeter, we no longer have the option of seeing all the traffic. How do you get the context of what is happening in your physical, virtual and cloud services? Just getting sample data is not enough anymore! This session will discuss how to get a real-time look into not only the on-prem traffic, but all your traffic – no matter where it lives. This session will look at how we are evolving from only feeding segments of traffic to our tools, to providing better, enriched data instead.

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

Scripps I

A Forensic Look at Windows® 10 Timeline Using SQL Queries to Exploit the Data
Rob Attoe, CEO, Spyder Forensics

Windows 10 introduced a new feature named "Timeline" which has seen enhancements in subsequent updates to the Operating System in 2018~2020. During this session we 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 firsthand look at the SQLite database containing all the artifacts while gaining an understanding of the cloud-based synchronization issues.

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

Scripps II

Industrial Control System Security: Protecting the Systems That Control Our World
Michael Sitler, Enterprise Security Business Architect, PPL Corporation

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

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

Canyon

RECON LAB
Jason Roslewich, CEO, SUMURI LLC

This demo will take attendees through RECON LAB, the only full forensic suite designed natively onthe Mac platform to harness the power of a Mac. Access over 270 timestamps and all Apple Extended Metadata for Mac investigations and automate the analysis of Windows, iOS, Android, RAM, Google and (of course, Mac). RECON LAB has an exponential number of reporting options including the first WYSIWYG report editor with chronological reporting.

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

Shore

Cybercrime Driven by Cryptocurrency
Johnmichael O'Hare, Director, Sales & Business Development, Cobwebs Technologies

Cybercrime orchestration in the deep and the dark web is fueled by Cryptocurrency. This session will demonstrate how to find Cryptocurrency wallet footprints over the deep and dark web and link IT cybercriminal groups with a goal to identify the source.

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

3:15pm – 4:15pm

Grande D

WhatsApp Forensics: Evidence Hide-and-Seek

Rene Novoa, Account Executive, Oxygen Forensics

WhatsApp is, without a doubt, the most popular messenger in the world with over 1.5 billion users globally. Thus, extracting complete evidence from WhatsApp Messenger is essential for any investigation. This session will look into all possible sources where WhatsApp data might be stored (mobile devices, computers, cloud) and present our exclusive method of WhatsApp data extraction directly from the WhatsApp Server. Moreover, the presenter will guide attendees through the process of WhatsApp backups decryption offering the alternative decryption method via phone number. Finally, the presenter will explain how to extract WhatsApp data from a locked mobile device using a WhatsApp QR token from a PC.

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

Grande E

2020 Information Security Risks and Trends

Eric Hlutke, Sr. Director and Chief Security Architect, Teradata

2020 by all accounts promises to be an active year. During this talk, we will explore some of the trending security risks forecasted in the mobile, insider threats, AI, Election Voting and Cloud computing space. We will end with pragmatic directions to begin the journey to address and educate you and your company on the risks and chart a path forward.

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

Tuesday, March 10 (continued)

The 2020 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 ● Sponsor Demo

3:15pm – 4:15pm (continued)

● **Scripps I**

Fake or Genuine? Forensically Authenticating Emails
Arman Gungor, CEO, Metaspike

Email evidence often plays a central role in legal proceedings, and fraudulent emails being passed as legitimate electronic evidence has become an increasingly common issue. Proving the authenticity of emails is no easy task for forensic examiners. The presenter will discuss data points that can be used to increase our confidence in legitimate emails and spot fraudulent ones. In this session, attendees will learn: How to preserve email evidence to facilitate forensic authentication; Common patterns to look for in fraudulent emails; and How to locate red flags efficiently in large data sets.

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

● **Scripps II**

Deconstructing Threat Intel
Jeff Marshall, CISO, DATASHIELD, an ADT company
David Norlin, Director, Threat Intelligence & Security, DATASHIELD, an ADT company

There are commonly held beliefs about threat intelligence and how it solves defense in depth problems and cures security issues. Rarely does this take into account knowledge of one's own environment. The industry currently fixates on security from an offensive perspective while neglecting internal defensive posture and measures. Understanding applications, practices and architecture are ignored for shiny tools, "hacking" coolness leading many security teams to suffer from an identity crisis. We plan to show the misconceptions and how to build a base foundation before spending time acquiring costly threat intel platforms. The speakers draw from extensive knowledge of the topic to help organizations start small and build a manageable threat intelligence program. We will utilize case studies as examples from real (security operations and military history. As a managed SOC we utilize several anonymized customer examples, lessons learned internally, and past experiences to illustrate and design an effective program. The speakers will also discuss common pitfalls of new threat intelligence consumers and how to avoid them.

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

● **Canyon**

From the Crime Scene to the Courtroom: Using Analytics to Analyze Mobile Forensic Data and Overcome "The Big Data Challenge"
Tanner Bokor, Regional Marketer, MSAB

One of today's biggest challenges for investigators, forensic examiners and others is to sift through and make sense of the huge volumes of data found on mobile devices. Having tools that can recover the digital evidence quickly is paramount and enables investigators to view it in a way that is understandable and be easily shared with other parties to act upon, whether in triage at the scene of a crime, in prosecution, or elsewhere. This session will introduce the latest improvements in MSAB's XAMN suite of analytical tools where you will learn how to harness the powerful filtering and visualization capabilities to find the artifacts you are looking for.

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

● **Shore**

Forensic Explorer — Advanced Forensic Software
Graham Henley, Director, GetData Forensics
John Thackray, Vice President, GetData Forensics USA

Forensic Explorer - Command Line, (An Automated, Repeatable Forensic Processing to Eliminate the Backlog)

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

4:30pm – 5:30pm

Grande D

APFS Imaging Considerations for Forensic Examiners

Jason Rafferty Roslewicz, Chief Executive Officer, SUMURI LLC

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

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

Grande E

Forensics in the Cloud

Dave Ryberg, Director of Truxton Sales, Probity/Truxton Forensics
Paul Muessig, Chief UI Architect, Truxton Forensics

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

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

Scripps I

What Skills Shortage? Bridge the Gap with Breach and Attack Simulation

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

This session is about how knowledge of your cybersecurity products, processes, and people will make you more powerful. Attendees will take a journey through the entire path of an attack scenario, diving into the technologies meant to protect you and how they are meant to work. Next, it will look at new technologies being engineered to help attendees perform deep assessment of their deployed security controls and highlight gaps that they can then work to fill. We will explore methodologies that are meant to help attendees perform these assessments and track their coverage as they progress.

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

Scripps II

Investigating Cyber Attack Cases

Brian Carrier, CTO, Basis Technology

Forensics groups in both law enforcement and industry are getting called on to perform more investigations into intrusion and cyber-attack cases. These types of investigations require a different focus and approach. This session will cover: The basics of investigating computers for intrusions; a Framework for approaching the problem; and Types of data to look for in the process.
In addition, the session will share tools that can be used during the investigation and show some examples using free software.

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

Canyon

Macquisition Triage and Live Collection Demo

Stephanie Thompson, Solutions Engineer, BlackBag Technologies

You asked for it! Come see if the newest capabilities in Macquisition to include the new triage functionality! If you are a new user or thinking about using Macquisition, we will also show how to do a live collection.

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

Wednesday, March 11

The 2020 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** **Sponsor Demo**

8:00am – 9:00am

Grande D

Early Riser Session: The Dark Web & Crypto Currency Investigations

Joe Saar, Detective, Costa Mesa Police Department
Rahul Gupta, Senior Trial Deputy, Orange County District Attorney's Office

Under the cloak of darkness, criminals are using tools for privacy and anonymity to commit a wide range of crimes on the Dark Web using Crypto Currency. During this session, attendees will learn some investigative tips and tricks to combat this new way of committing old crimes.

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

9:15am – 10:15am

Grande D

Digital Evidence from Social Networking Sites & Smartphone Apps

Julie Lewis, President & CEO, Digital Mountain, Inc.
Cynthia Navarro, High Tech Investigator, Digital Mountain, Inc.

In 2018, more than 77 percent of the United States population had a social media profile. Mobile device usage for social media has increased to 91% of social channel accesses in 2018 according to Marketing Profs. Many technology thought leaders believe social networking will displace traditional email as the leading communication medium. This session will provide a practical walkthrough of preservation of top social media sites and how to effectively utilize tools for evidentiary collection across the Web, PCs/desktops and smart devices. We will look at social media apps on smartphones and what digital evidence exists compared to what can be found on the cloud. We will also explore innovations in emoji/avatar Apps such as Bitmoji.

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

Grande E

AI's Role in Enabling Next Gen Forensic Defense and Protection

Rick Grinnell, Founder and Managing Partner, Glasswing Ventures
Salvatore Stolfo, Professor of Computer Science, Founder and CTO, Columbia University & Allure Security
Candan Bolukbas, Chief Technology Officer & Co-Founder, NormShield
Tyler Carbone, CSO, Terbium Labs

Leading experts explore the latest trends and best practices in leveraging AI in the world of Cybersecurity and Forensics. This panel of leading technology executives and academics will discuss the role that state of the art AI plays in identifying the holes and tracking compromised credentials. The panel will provide an overview as well as real-world use cases on where AI is being used in the Dark Web and insights on assessing cyber risk and forensic analysis.

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

Scripps I

New Ways to Commit Crimes...and New Ways to Solve Them (with cars)

Andrea Amico, Founder, Privacy4Cars

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

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

9:15am – 10:15am (continued)

Scripps II

Managing Security Risks from the Department Level to the Boardroom
Karlene Apelt, Information Governance Program Manager, NVISNx
Nandita Narla, Information Governance Program Lead, NVISNx
Gagan Sarawgi, Information Systems Manager, NVISNx

By 2020, 100% of large enterprises will be asked to report to their board of directors on cybersecurity and technology risk at least annually. The question is what's the best way to get the message across. Managing security risks may start at a department level, but by providing a global view of the information assets across the enterprise, we can enable business leaders to make better decisions and then take action as to what to keep, what to dispose of and how to better protect their information assets. Business leaders need to be in control of its data, not the other way around. The session will show advanced capabilities for monitoring and protecting critical data, enabling contextual threat hunting, enhanced business intelligence for complying with complex regulations, like GDPR and CCPA, retention schedules and privacy rules and how best to present a global view of cybersecurity and technology risks to the Boardroom.

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

Canyon

Ciphertex SecureNAS
Jerry Kaner, Founder & President, Ciphertex Data Security

Increase throughput and profitability with better tools. As data increases at an exponential rate, it is imperative to have the tools that keep pace with the workload and ever-increasing security threats. Ciphertex Data Security®, the leading encrypted storage solution provider, introduces a Series of new portable NAS devices that will not only outperform current systems, but change the way you work with increased throughput and USB quick connect networking. Build larger teams, move more data and reduce time in the field for increased profitability. See the New Ciphertex SecureNAS series at Techno Security & Digital Forensics Booth# 308 as we take a deeper dive into the workflow in the field.

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

10:30am – 11:30am

Grande D

Reinventing the Standard Operating Procedure for Corporate Forensics
Jerry Bui, Executive Director, Digital Forensics, Lighthouse

When completing a digital forensics investigation in a corporate setting, you're often working against the clock to deliver results to your executive stakeholders. This session will share a number of innovative methodologies that help teams meet the demands of their customers while completing investigations as efficiently as possible. How to kick off investigations with a better starting point by focusing on analysis, as opposed to collection; How automation can help acquire remote images and reduce processing time; How to access critical cloud data; and More.

Target Level: Intermediate
Target Audience: Corporate/Private Sector

Grande E

Securing the Digital Homeland: The Department of Homeland Security and the Cyber Security Landscape
Joseph Oregon, Cybersecurity Advisor, Region IX (S. CA), Department of Homeland Security

This session will discuss the cyber security landscape, including current and emerging threats that attendees need to be aware of today and in the near future. The presenter will explore the role of the Department of Homeland Security and its Cyber Security Advisor (CSA) program designed to protect cyber components essential to the nation's critical infrastructure and key resources, state and local governments and private entities. Attendees will learn how they can collaborate with the CSA program on cyber preparedness, risk mitigation, incident & information coordination and cyber policy promotion & situational awareness.

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

Wednesday, March 11 (continued)

The 2020 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** ● **Sponsor Demo**

10:30am – 11:30am (continued)

● **Scripps I**

Intro to Blockchain & Crypto Currency Investigations Lab
John Wilson, President, HaystackID, LLC

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

Note: This lab is BYOL (Bring your own laptop) however any basic laptop that can browse the internet will suffice.

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

● **Scripps II**

Rogue Device Mitigation
Yossi Appleboum, CEO, Sepio Systems

While the industry is focused almost entirely on software protection against cyber-attacks, one of the greatest threats resides in rogue or corrupt hardware devices that are present in almost every computing network and infrastructure. From the doctored motherboard chips on our servers that have been corrupted along the supply chain to compromised peripheral devices, mobile phones and USB drops, hardware vulnerabilities represent a target rich environment for cyber criminals leveraging a variety of threat exploits. Citing examples occurring recently in the International server manufacturing supply chain, IP theft by disgruntled employees, and data leaks at a Fortune 20 bank, the presenter will explain how to detect, prevent, and protect information systems from hardware-based attacks.

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

● **Canyon**

Collaborative Review Using Intella Connect
Rob Attoe, CEO, Spyder Forensics

Large scale investigations require a collaborative approach to examine data quickly and efficiently, which leads to improved productivity and workflows. Intella Connect provides a web-enabled, collaborative platform that gives a team of examiners the ability to review more cases at the same time. During this session, we begin with simple configuration settings followed by workflows in collaborative review using the web-based client. Topics of discussion include: keyword search, document analysis, tagging, exports, case management and assignments, reviewer functions and case configuration considerations, case analysis, data culling techniques, email threading analysis and review, and batch coding and document reviewing options.

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

● **Shore**

Digital Video Evidence: The Quest for Accuracy and Competence
Jessica Callinan, Investigative Technician, San Diego County District Attorney's Office, California
Renato Nerida, Physical Security Program Analyst, University of California San Diego Police Department

This session offers you a fundamental understanding of forensic video analysis. Get thinking about the material value of video evidence and the shortcomings if not properly trained to handle it. Also covered will be what to keep in mind when faced with retrieving digital video evidence, processing it, playback challenges as well as delivering the video evidence for potential court proceedings.

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

1:30pm – 2:30pm

Grande D

Mitigating Risk Through Threat Hunting

Steven Konecny, Partner, Forensic Security Solutions
Dave Thompson, Partner, Forensic Security Solutions

What do many of the top security breaches over the last few years have in common? Most of the victim enterprises spent millions of dollars on security, had SOCs, firewalls, IDFs and anti-virus systems. However, had they taken a more proactive approach they may have been able to identify the "hackers" within their systems before data was exfiltrated or Ransomware was installed. This session will discuss techniques used in threat hunting, identify products both open source and commercial that will assist the practitioner and review the areas and artifacts left behind by hackers that will show potential indicators that a system may have been compromised

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

Grande E

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

Charles Giglia, Vice President, Digital intelligence, Inc.

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 attendees determine if CCleaner was executed on a computer and what data you will see once these important artifacts have been deleted

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

Scripps I

The Butterfly Effect Theory — Lone Wolf Shooter Syndrome

Johnmichael OHare, Sales Director, Cobwebs Technologies

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

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

Scripps II

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. This session will present some of our findings from years in the field and discover the nexus of pragmatic threat intelligence, supply chain security and vendor risk management. Blind faith is no longer an option.

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

Wednesday, March 11 (continued)

The 2020 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** ● **Sponsor Demo**

1:30pm – 2:30pm (continued)

● **Canyon**

Graykey & Apple iOS/Devices
Jonathan Oszust, Account Manager for Midwest & West Coast/Canadian, Grayshift

This demo will explain how Grayshift is able to use its next generation access forensic tool called Graykey to bypass today's locked iOS devices. Grayshift will explain why today's iOS devices are so secure and what are the challenges for today's law enforcement & tech companies from accessing this sensitive data that sits within these iOS devices. Grayshift will also provide a live demonstration regarding their Graykey and go into greater detail about the differences between iOS versions, models, and also discuss the differences between BFU & AFU.

Law Enforcement, DA's & AG's Office (NO PUBLIC DEFENDERS) Govt., Federal and Military attendees ONLY

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

3:15pm – 4:15pm

● **Grande D**

Investigating Fake Digital Photos
Chester Hosmer, Author, Python Forensics, Inc.

The global impact resulting from the distribution of doctored digital photographs has reached an epidemic proportion. These digitally altered photos are distributed through social media, news outlets, traditional web resources and are making their way into the mainstream media. The impact of these photos can dramatically change the way people think, act, react, believe and can ultimately cause harm. At the simplest level, they represent visual fraud. During this session, the presenter will convey real examples along with the resulting impacts that have already occurred. Most importantly, the presenter will demonstrate a new methodology rooted in the dark art of steganography that can actively identify these fraudulent photos and even trace their origins back to their creators.

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

● **Grande E**

Cruising on a Security Data Lake: Solving Big Data Challenges in SECOPS
Charles Herring, CTO, WitFoo, Inc.

Researchers at WitFoo in conjunction with The University of Chicago and representatives from Law Enforcement, US Military and Fortune 500 organizations conducted more than 2000 controlled experiments on production networks from 2016 through 2018 to establish a Big Data pipeline for use in CyberSecurity Operations that allows for the application of investigative workflows and indicators of compromise in near realtime as well as providing for retrospective analysis of the complete data stack when new insights and indicators are made available. The first section of the session will evaluate the strengths and limitations of Big Data technologies including Elasticsearch, Splunk, Hadoop, Kafka, MySQL NDB, Cassandra, NoSQL vs RDBM as well as pipeline philosophies including streaming and batch processing. The second section will outline the specific approaches that are used in the discovered pipeline. Detailed demo and code will be provided to illustrate adaptive and retrospective parsing, event generation and data evolution. The third section will provide a demonstration of the pipeline in use to detect emerging threats and to retrospectively find threats missed historically. Upon completion of the session, attendees will understand the philosophies, components and steps in creating an effective big data pipeline that addresses the challenges in Cyber Security Operations.

Target Level: Intermediate
Target Audience: Corporate/Private Sector

3:15pm – 4:15pm (continued)

Scripps I

Protecting Active Directory: Detecting Insider and Privileged Attacks

Derek Melber, Technical Director, North America, Alsid

Active Directory is the keystone for nearly every enterprise in the world. With this being said, it is constantly under attack, especially from inside the organization. Unfortunately the built-in capabilities to monitor, track, or detect these attacks is minimal... some would even say non-existent. In this session, the presenter will go over some of the most prevalent attacks and show you how attendees can, in real-time, detect these attacks. When done with this session attendees will have an immediate solution to discovering and knowing when your AD is under attack.

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

Scripps II

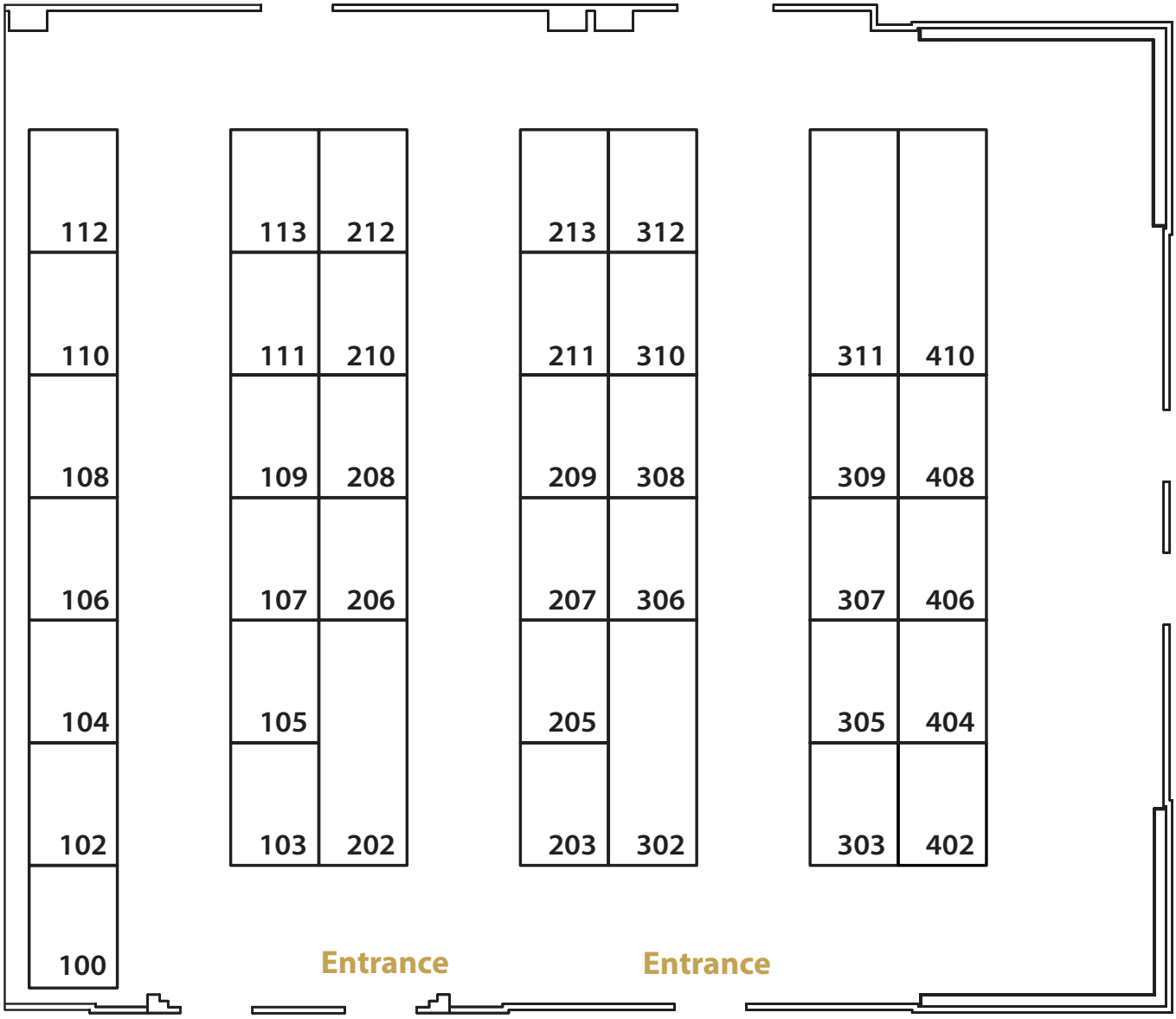
Live Forensics in Locked Computers

Kristopher Carver, Technical Director, BlueRISC Inc.

Performing live memory analysis is an increasingly critical component in a forensic investigation. Existing solutions for obtaining an image of the system's live memory (DRAM) require, however, access to a live, unlocked computer. But what do you do when you don't have the password? How can you guarantee that the acquisition process was not compromised? How do you make sense of all the information contained in a raw memory dump? This session will introduce a new hardware-assisted tool-kit to solve these problems. We will describe and demonstrate the solution to gain access to a locked computer, provide an overview of the options for imaging live memory under various scenarios, and go into depth on the reverse engineering and analysis techniques to make sense of the gigabytes worth of live information, including kernel and user-level software and data structures.

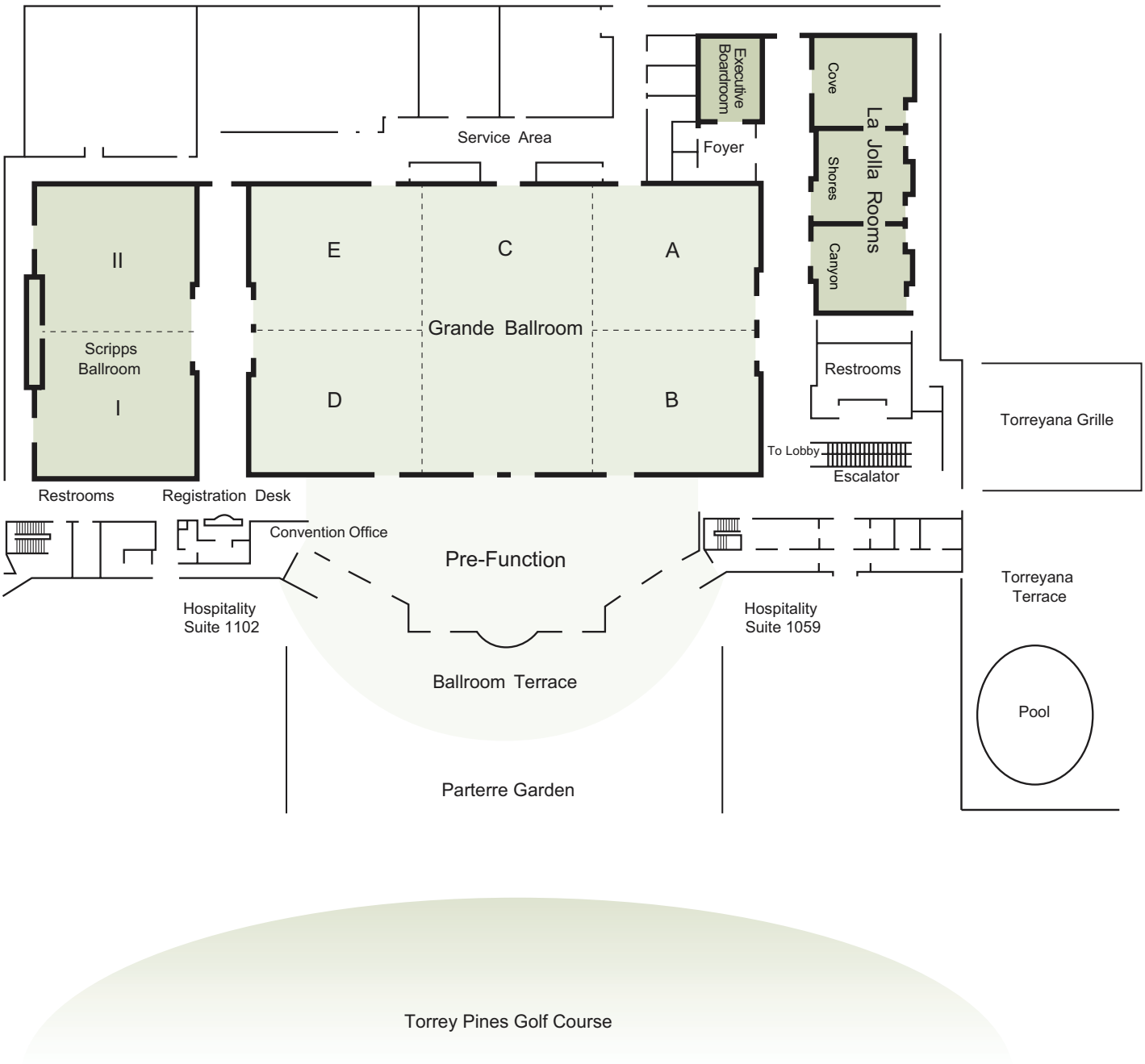
Target Level: All Levels
Target Audience: Corporate/Private Sector, Government, Investigators, Law Enforcement/Police

Grande Ballroom A/B/C



Pre-Function

(Breakfast & Lunch Buffets)


Service Area
Executive Boardroom
Foyer
Cove
La Jolla Rooms
Shores
Canyon
II
E
C
A
Grande Ballroom
Scripps Ballroom
I
D
B
Restrooms
To Lobby
Escalator
Torreyana Grille
Restrooms
Registration Desk
Convention Office
Pre-Function
Hospitality Suite 1102
Hospitality Suite 1059
Torreyana Terrace
Ballroom Terrace
Pool
Parterre Garden
Torrey Pines Golf Course

AccessData

Booth 105

Orem, UT, USA
(480) 361-3513

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 Technology Partners

Booth 406

Elk Grove Village, IL, USA
(847) 952-6911

www.acetechpartners.com

Ace Technology Partners is a 37-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 2GIT, Army_ADMC3 and others. Come and see our latest FORCE™ Workstations and CipherFORCE™ Password Cracking Appliances!

Argent Software

Booth 100

New York, NY, 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 108

Vancouver, BC, Canada
(888) 540-2010

www.atola.com

FAST FORENSIC IMAGING EVEN WITH DAMAGED DRIVES! Get more digital evidence faster with Atola Technology's INSIGHT FORENSIC and TASKFORCE forensic imagers. The first and only forensic imagers that can get data from both good and even damaged 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 104

Los Angeles, CA, USA
(310) 625-9252

www.belkasoft.com

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

Berla

Booth 410

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 311

San Jose, CA, USA
(408) 513-1825

www.blackbagtech.com

BlackBag Technologies develops innovative forensics acquisition, triage, and analysis software for Windows, Android, iOS, and MacOS 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.

Centripetal

Booth 110

Herndon, VA, USA
(949) 291-5705

www.centripetalnetworks.com

Centripetal delivers intelligence-driven security. Centripetal invented the Threat Intelligence Gateway and leverages its technologies to deliver CleanINTERNET, a comprehensive intelligence-led cyber service. With Centripetal, customers can persistently prevent over 90% of known threats with intelligence applied in advance. Centripetal's technology is protected by over 50 US and international patents.

Ciphertex Data Security

Booth 308

Chatsworth, CA, USA
(818) 773-8989

www.ciphertex.com

Ciphertex Data Security® is a leading encrypted storage solutions provider. Our new Ciphertex SecureNAS® systems are the next step in the long history Ciphertex has working with Forensics and Law Enforcement. Taking input from our customers and leading forensic product providers, the Ciphertex SecureNAS is tailor made for field work.

Cobwebs Technologies

Booth 307

New York, NY, USA
(201) 937-9707

www.cobwebs.com

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

Digital Intelligence

Booth 111

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

www.digitalintelligence.com

Digital Intelligence continually innovates the design of forensic hardware and lab solutions. With an array of forensic workstations, DI allows for tailored customization to meet customer demands. Additionally, we offer training on general forensics and the majority of the industry software/hardware, as well as providing Digital Forensic and eDiscovery services.

EDAS FOX

Booth 107

Largo, FL, USA
(727) 657-1526

www.edasfox.com

For the past 16 years we have proudly provided and supported our EDAS FOX line of Forensic Computers to thousands of customers worldwide. Law enforcement, military and corporate clients trust EDAS FOX. Our 3 year warranty ensures your EDAS FOX will provide years of reliable examinations.

EDEC Digital Forensics

Booth 208

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

www.edecdf.com

Next-generation RF shielding — EDEC Faraday 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 OffGrid™, a new product line with advanced features for a new generation of evidence security.

FINAL DATA INC.

Booth 109

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 203

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

www.forensiccomputers.com

Forensic Computers, Inc (FCI) has been engineering and constructing premium, custom-made forensic 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 306

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.

GetData - Forensic Explorer

Booth 212

Manhattan Beach, CA, USA
(310) 740-5137

www.forensicexplorer.com

GetData Forensics was founded in 2002. GetData's aim is to provide cutting edge and cost-effective software, support and training to both law-enforcement and the corporate sectors to assist in the fight against crime. GetData is known best for its forensic tools Mount Image Pro and Forensic Explorer.

Grayshift

Booth 305

Atlanta, GA, USA
(833) 472-9539

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.

IntaForensics - Lima

Booth 404

Nuneaton, United Kingdom
+44 02477 717780

www.intaforensics.com

IntaForensics are an ISO/IEC 17025 accredited digital forensic provider and creator of Lima; the multi-award winning digital forensic case management system. IntaForensics is also a provider of MSSP, VCISO, Incident Response, PFI, QSA and a range of consultative services.

LEVA

Booth 210

Fuquay Varina, NC, USA
(540) 842-1742

www.leva.org

Provides the global standard of digital multimedia evidence training. The only organization in the world that provides court-recognized training in video forensics that leads to certification.

Logicube

Booth 103

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

www.logicube.com

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

Magnet Forensics

Booth 302

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.

MOS Equipment

Booth 312

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

Booth 309

Arlington, VA, USA
(703) 996-4549

www.msab.com

MSAB pioneers mobile forensic technology for mobile device examination. Our tool suite — XRY, XAMN and XEC — is used in over 100 countries to investigate crime and fraud, gather intelligence and fight corruption. MSAB's sole focus is secure forensic extraction, analysis and management of data from mobile devices.

OpenText

Booth 205

Austin, TX, USA
(905) 762-6352

www.opentext.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.

Oxygen Forensics

Booth 207

Alexandria, VA, USA
(877) 969-9436

www.oxygen-forensic.com

Oxygen Forensics is the leading global digital forensics software provider, giving LE, federal agencies, enterprises access to critical data and insights faster than ever before. Specializing in mobile devices, cloud, drones and IoT data, Oxygen Forensics provides the most advanced data extraction and analytical tools for criminal and corporate investigations.

Paraben

Booth 106

Aldie, VA, USA
(801) 796-0944

www.paraben.com

Paraben has been a technology innovator for 20 years. Paraben's solutions work with smartphones, cloud, IoT, computer, email, and gaming investigations. Paraben provides a unified software interface for all types of digital data. From start-to-finish, Paraben offers solutions that can build new capabilities into any digital investigation.

Silicon Forensics

Booth 209

Pomona, CA, USA
(909) 632-1797

www.siliconforensics.com

Silicon Forensics was founded in 1992 with a mission to serve the digital forensics community. Today, we aim to modify forensic acquisition technology, defy industry conventions and provide intelligent digital forensic hardware solutions to help create a safer world.

Sumuri

Booth 303

Camden Wyoming, DE, USA
(302) 570-0015

www.sumuri.com

SUMURI is known for developing innovative and forward-thinking forensic software, hardware, training, and services. SUMURI's core mission consists to provide the forensic community with unique and relevant digital forensic solutions while adhering to our core values of honor, integrity, loyalty, positive attitude, dedication and most important above all, altruism.

Susteen

Booth 202

Irvine, CA, USA
(949) 341-0007

www.datapilot.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 213

Vienna, Austria
+43 699 132 375 43

www.t3k-forensics.com

T3K-Forensics is an Austrian based, B2G focused technology company that specializes in forensics services and software development. T3K-Forensics provides certified witness expertise for public prosecutor's office, training courses in mobile forensics and advanced analytical solutions to LEAs across Europe. We combine our forensics expertise with AI, to accelerate forensics workflow.

Teel Technologies

Booth 408

Norwalk, CT, USA
(203) 855-5387

www.teeltech.com

Since 2006, Teel Technologies has delivered leading digital forensic technologies, training and services to the worldwide forensics community. Almost 15 years later, our focus remains focused on bringing effective solutions and teaching best practices to the digital forensic investigator. Come see our complete collection of tools for field and lab.

Truxton Forensics

Booth 206

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.

Vound Software

Booth 113

Scottsdale, AZ, USA
(443) 221-0717

www.vound-software.com

Vound is a leading global vendor of technology used for forensic search, e-discovery, and information governance. Our unique technology utilizes cluster maps, timelines, and link graphs to significantly reduce the time and costs organizations normally need to carry out digital investigations, audit requests, and eDiscovery.

Thank You to Our 2020 Advisory Board!

Dennis W. Kuntz – Manager, Vulnerability Management, Amazon

Julie Lewis – President & CEO, Digital Mountain, Inc.

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

Nandita Narla – Information Governance Program Lead, NVISNx

Peter Phurchpean – Investigator, Computer Crimes Investigation Unit, California Highway Patrol

Joseph Pochron – Senior Manager, Forensic & Integrity Services, Privacy & Cyber Response, Ernst & Young LLP

Tamara Poelma – Program Manager/Digital Forensics Investigator, Hi-Tech Crimes & Surveillance Unit, State of California Department of Toxic Substances Control Office of Criminal Investigations

Matthew Rosenquist – Cybersecurity Strategist, Independent

Erich Schmidt – High-Tech Investigator, Government Task Force

John Simpson – Assistant Director, Digital Forensics, Australian Taxation Office

Thank You to Our 2020 Industry Supporters!

Cyber Center of Excellence

DIGITAL FORENSIC COMMUNITY

ENTERPRISE SECURITY

FORENSIC FOCUS
FORENSICFOCUS.COM

GOVCIO OUTLOOK

MY TECHMAG

THE CYBER SOCIAL HUB

WSC
Women's Society of Cyberjutsu

PLATINUM SPONSORS

BERLA

BlackBag®

DATAPILOT

MAGNET FORENSICS®

GOLD SPONSORS

ARGENT

CIPHERTEX® data security

COBWEBS TECHNOLOGIES

EDEC

FCI Forensic Computers Incorporated

geotime®

GetData FORENSICS

GRAYSHIFT

LEVA INTERNATIONAL, INC.

Logicube®

MISSION DARKNESS Made By MOS Equipment MOS equipment mountain. ocean. sky. www.mosequipment.com

MSAB

opentext™

OXYGEN FORENSICS

SiliconForensics

SUMURI

T3K-Forensics

TRUXTON

Vound

SILVER SPONSORS

ACCESSDATA

ACETECHPARTNERS

Atola TECHNOLOGY

AVAIL Forensics

Belkasoft forensics made easier

Centripetal

Digital Intelligence®

FINAL DATA Forensic Acquisition, Analysis and Data Recovery Solutions

HTCI EDAS FOX LLC

IntaForensics

paraben® corporation paraben.com

TEELtechnologies