Day 1 Morning Agenda

Lecture | Lab | Cert | Prosecutor 3 Day

Conference Info

Featured Speakers

Day 1 Morning Sessions 1 and 2

Day 1 Afternoon Session 3 & Judicial Panel

Day 2 Morning Sessions 4, 5, and 6

Room	SESSION 1 10:00 AM - 11:15 AM	SESSION 2 11:30 AM - 12:45 PM
101	Tips & Tricks	
102	The Path of Child Sex Abuse Images: From Victimization to Restitution	Sextortion: Findings from NCMEC's Cyber Tipline
103	DVR Triage: Best Practices For Recovering Digital Video Evidence	Interview & Interrogations
104	Terrorism & Technology	Internet Cafes/Sweepstakes Gaming
105/6	4th & 5th Amendments	
107	OsTriage	
108	Navigating Social Media	Dark Web Investigations
111	Magnet Forensics Demonstration	SysTools Demonstration
112	Cell Phone Forensics	Extracting Cloud Data Using Tokens Obtained From Cell Phones
113	Law Enforcement's Role in Cybersecurity	Processing Windows Event Logs for Timelining Criminal Cases
115	Searching Facebook and Instagram	
116	MDEC - Report Writing and Testimony	
117	Microsoft and TASER Leverage the Cloud to Drive Safer Communities	Microsoft Online, Safety & Services Overview
201		Recovery of Video Evidence Using DVR Examiner
202	Introduction to Cyber Crime and Computer Forensics	Collection of Digital Evidence – With Search Warrant

LUNCH - Going Dark - A Panel DIscussion

TIFFANY BALLROOM - 1:00 PM - 2:15 PM

Session 1 | 10:00 AM: 11:15 AM
Descriptions

Tips & Tricks
Room: 101 | **Type**: Lecture

The Menz Brothers & Kip Loving class has been commonly known as the "tips and tricks" class for Internet investigations and digital forensics. The class will present and demonstrate current software and techniques for both investigation and forensic examinations that are not commonly known or are newly discovered or written. They will also present items that will become problems in the future for investigations. Those who attend the class also leave with a DVD of most of the software, web site.

This session continues in Session 2.

Instructors: Michael Menz | Detective Kipp Loving

The Path of Child Sex Abuse Images: From Victimization to Restitution
Room: 102 | **Type**: Lecture

Child sexual abuse images have a lifecycle that touches representatives from many agencies throughout the world as we work collaboratively to combat this problem.Come learn about the path these files take from a victim-centered standpoint,and how your help and participation in the "chain" is pivotal to rescuing children featured in child sexual abuse images.The role of NCMEC,how they interact and are connected,along with their resources for investigators, will be discussed in depth.

Instructor: Rebecca Sternburg

DVR Triage: Best Practices For Recovering Digital Video Evidence
Room: 103 | **Type**: Lecture

Investigators will learn what tools they need to capture and preserve digital video evidence from a crime scene DVR and get it to Court. You will learn to assess your options for retrieving the best possible evidence for your case. Discussion will cover: investigative tools, capturing video, calculating date & time offset, getting surveillance video to play, proprietary video players and CODECs. Observe a live demonstration where surveillance video is captured and processed in the classroom.

Instructor: Paul Melaragni

Terrorism & Technology
Room: 104 | **Type**: Lecture

Islamic Terrorism, the recruitment methods, and their use of available technologies and tools

Instructor: Majid Hassan

Session 1 | 10:00 AM: 11:15 AM
Descriptions

4th & 5th Amendments
Room: 105/6 | **Type**: Lecture

These sessions provide both the governmental and ACLU perspective on the latest issues in 4th and 5th Amendment law. Topics that will be discussed include evolving expectations of privacy in the digital age, the "third party doctrine," ex ante restrictions in search warrants, and compelled production of electronic "keys" to encrypted data.

Panelists: Honorable Ron Hedges, ADA Tom Ralph, Jessie J. Rossman, Esq.

osTriage
Room: 107 | **Type**: Lab

This hands-on lab will provide instruction on osTriage, where to get it, how to use it, and how it can enhance on-scene previews to give you the most information in the shortest amount of time. osTriage will quickly find, extract, and display key information from a computer which will enable you to get a better first interview of your subject and conduct a better search of the subject premises.

Instructor: Jeffrey Rich

Navigating Social Media
Room: 108 | **Type**: Lab

In this lab we will become familiar with the online interfaces of Twitter© and Facebook© as well as the language of these platforms.

Knowing how to set up Twitter© lists can help you narrow your focus and searches. We will also explore free online tools that integrate these two social mediums which can provide you a more productive environment.

Instructor: Aaron Kravitz

Cell Phone Forensics
Room: 112 | **Type**: Lab

Learn about techniques used to examine popular smartphones, specifically iOS- and Android- based devices, including methods used to bypass / recover security codes and swipe patterns. Attendees will learn how to recover vital chat data from messaging apps and correlate common data between multiple devices via instantly plotted connection diagrams, timelines, and geomaps.

Instructor: Wil Hernandez

Session 1 | 10:00 AM: 11:15 AM
Descriptions

Law Enforcement's Role in Cybersecurity
Room: 113 | **Type**: Lecture

In this lecture, students will learn about cyber terminology and cyber threats facing law enforcement today, such as the direct threats by hacktivist groups like Anonymous. Students learn how cybercriminals are employing the Internet to attack state and local governments and to facilitate organized crime networks. Adapted from NW3C's Cybersecurity 235 - Basic Network Intrusion Investigations http://www.nw3c.org/training/Computer-Crime/126.

Instructors: Cynthia Gonnella | Mike Stern

Searching Facebook and Instagram
Room: 115 | **Type**: Lab

Facebook is the largest worldwide social media website and contains a substantial amount of potential investigative information. Facebook information can be searched in three separate and distinct ways. One method is to use Facebook graph search, which uses specific targeted terms that, when used correctly, can show investigative material. The instructor will demonstrate how graph search works, and explain how syntax—the structure of the search keywords and phrases—is vital to a successful search. The second method is to use URL manipulations. Once a Facebook profile has been identified, these URL manipulations can show content from this target, such as photo comments, video likes, and comparisons with friends. These URL manipulations are specific and offer information beyond what can be found simply by looking at someone's profile. The third method uses Google advanced and Boolean operators to search on Facebook in a more broad sense. Constructing a good keyword string is key to ensuring that investigative material is found. The instructor will demonstrate examples of specific syntax that should be used. Additionally, searcing techniques for Instagram will be addressed, including searching by name, username, keyword, and even geographical area.

This session continues in Session 2.

Instructors: Lauren Wagner | Dean Chatfield

MDEC (Module 2) (Report Writing)
Room: 116 | **Type**: Cert

The Massachusetts Digital Evidence Consortium (MDEC) will feature three modules of instruction toward MDEC digital evidence certification programs. Participants in this module will learn to communicate their digital evidence examination findings both orally through testimony, and on paper through quality export report writing. Successful completion of this module is a prerequisite for completion of the MDEC Certified Massachusetts Digital Evidence Analyst certification. The module consists of this training component as well as a practical component, which is satisfied by taking part in the MDEC Testimony Boot Camp.

Instructor: Massachusetts Digital Evidence Consortium

Session 1 | 10:00 AM: 11:15 AM
Descriptions

Microsoft and TASER Leverage the Cloud to Drive Safer Communities
Room: 117 | **Type**: Lecture

Body-worn and in-car video systems are some of the most important tools for law enforcement and the communities they serve - they help to solve crimes, increase transparency, and build trust in the community. For example, Axon cameras resulted in an 87.5% drop in complaints against officers for the city of Rialto, California, and the City of Pittsburgh Bureau of Police saw their numbers decrease by 74%. In this session you'll learn how Microsoft and TASER are leveraging the cloud to deliver breakthrough solutions for video capture, evidence management, analysis, and collaboration within agencies - all part of driving safer communities.

Instructors: Jeff King | Isaiah Fields

Intro and Computer Forensics
Room: 202 | **Type**: Cert

This session will include an introduction to the three day prosecutor course. In addition, this presentation covers the fundamentals of computer forensics, and discusses the many forensic artifacts that are useful to prove up a variety of criminal charges.

Instructors: Justin Fitzsimmons | Lieutenant David McSweeney

Session 2 | 11:30 AM: 12:45 PM
Descriptions

Tips & Tricks
Room: 101 | **Type**: Lecture

This session is a continuation from Session 1.

Instructors: Michael Menz | Detective Kipp Loving

The Art of Interview and Interrogation
Room: 102 | **Type**: Lecture

The interview, it can be argued, is the most important segment of police work. Interviews are conducted by every police officer, every day. How do you get the most out of the interview? How do you know who is telling the truth? How can you tell with any degree of certainty? This course will cover the basics on what all police officers need to know regarding the subject. The instructor will cover the constitutional issues involved in speaking with witnesses, complainants, and suspects. The proper setting, preparations to be made prior to interviewing, and formatting what needs to be done to accomplish the police officer's goal- the truth will be discussed. Law books state that eighty percent of guilty persons will confess to a crime, under the right set of circumstances. Why aren't we getting clearances like that? The course will deal with understanding and stopping denials. It will address the suggested way in order to record witness or suspect testimony, the reading of verbal, non-verbal, neurolinguistics and statement analysis. This course will afford the new officer a start in the complex art of interviewing and will improve the veteran officer's approach to this most necessary part of police work. The course will conclude with preparing the law enforcement professional to get the most out of the interview and be prepared to testify in court. The attendees will leave with the knowledge of how to conduct a proper interview and interrogation and how to get to the truth.

Instructor: Detective Sergeant Peter Curran

Cybercrime Trends and International Investigations
Room: 103 | **Type**: Lecture

This presentation will focus on current Cybercrime trends to include Business Email Compromise Fraud and Ransomware. It will also incorporate two case studies on conducting international investigations.

Instructor: Assistant to the Special Agent in Charge John Liau

Internet Cafes & Sweepstakes Gaming
Room: 104 | **Type**: Lecture

Commercial gambling enterprises masquerading as "internet cafes" are spreading across the US. This presentation will focus on the facts which arose in two criminal investigations of these cafes in Arizona and the statutory framework which resulted in felony convictions of the owner and manager of one of these operations in Arizona state superior court in November of 2015.

Instructor: Todd Lawson

Session 2 | 11:30 AM: 12:45 PM
Descriptions

4th & 5th Amendments
Room: 105/6 | **Type**: Lecture

These sessions provide both the governmental and ACLU perspective on the latest issues in 4th and 5th Amendment law. Topics that will be discussed include evolving expectations of privacy in the digital age, the "third party doctrine," ex ante restrictions in search warrants, and compelled production of electronic "keys" to encrypted data.

Panelists: Honorable Ron Hedges, ADA Tom Ralph, Jessie J. Rossman, Esq.

osTriage
Room: 107 | **Type**: Lab

This lab is a continuation from Session 1. Pre-registration is required for admittance into this lab.

Instructor: Jeffrey Rich

Dark Web Investigations
Room: 108 | **Type**: Lab

Attendees will learn the background of what the Dark Web is and where to find hiding criminals. The attendees will be able to identify the differences between the Dark Web and the Deep Web. They will learn how to get into the Dark Web and search for hiding criminals.

Instructor: Todd Shipley

Extracting Cloud Data Using Tokens Obtained from Cell Phones
Room: 112 | **Type**: Lab

Learn how to recover cloud data from mobile devices using the tokens or credentials collected during cell phone dumps.

Instructor: Rey Navarro

Processing Windows Event Logs for Timelining Criminal Cases
Room: 113 | **Type**: Lab

In this hands-on lab, students will use Fire-Eye Mandiant's Redline to collect and process data to tell a story of how files came to be on a particular machine. This skill is very important when working computer facilitated criminal cases. Students learn to timeline Internet history, file downloads, program installations, programs run, files accessed, and by what account. Instructed by experienced investigators. Adapted from NW3C's Cybersecurty 235 - Basic Network Intrusion Investgations course.

Instructors: Cynthia Gonnella | Michael Stern

Searching Facebook and Instagram
Room: 115 | **Type**: Lab

This lab is a continuation from Session 1. Pre-registration is required for admittance into this lab.

Instructors: Lauren Wagner | Dean Chatfield

Session 2 | 11:30 AM: 12:45 PM
Descriptions

MDEC (Module 2) (Report Writing)
Room: 116 | **Type**: Cert

This cert is a continuation from Session 1. Pre-registration is required for admittance into this cert.

Instructor: Massachusetts Digital Evidence Consortium

Microsoft Online, Safety & Services Overview
Room: 117 | **Type**: Lecture

This presentation will provide an overview of the major online services which Microsoft provides to customers including Outlook.com (Hotmail), OneDrive, Skype and XBox. For each service, you will learn what data may be available with the appropriate service of legal process, where and how to serve legal process, user notification policies, requirements for threat-to-life emergency requests, and response expectations.

Instructor: Tracy Ingle

Recovery of Video Evidence Using DVR Examiner
Room: 201 | **Type**: Lecture

Recovering video evidence from CCTV digital video recorders (DVRs) can be a difficult process, but it doesn't have to be. DVR Examiner is a software solution for acquiring video and metadata from CCTV DVRs in a forensically sound manner. In this session, we will demonstrate how to recover evidence quickly and easily from a DVR hard drive or forensic image. We will also briefly discuss the technical processes behind DVR Examiner.

Instructor: Brewster Rolland-Keith

Collection of Digital Evidence – With Search Warrant
Room: 202 | **Type**: Cert

This presentation explores the different types of search and seizure used in technology--facilitated child sexual exploitation (TFCSE) cases. The audience learns the differences between a consent search and a search warrant, and discusses applicable cases for each.

Instructor: Margaret M. Ogarek

Day 1 Afternoon Agenda

Lecture | Lab | Cert | Prosecutor 3 Day

Conference Info

Featured Speakers

Day 1 Morning Sessions 1 and 2

Day 1 Afternoon Session 3 & Judicial Panel

Day 2 Morning Sessions 4, 5, and 6

Room	SESSION 3 2:30 PM - 3:45 PM	Judicial Panel 4:00 PM - 5:30 PM
101	Wireless Technology	
102	Cybercrime Trends and International Investigations	
103	Bridging the Gap Between Computer and Mobile Device Forensic Examinations	
104	Survey of Gaming in Massachusetts - Casinos, Fantasy Sports and Sportsbetting	
105/6	ECPA/SCA	
107	Overcome Your Toughest Forensic Challenges with Cellebrite Advanced Investigative Services	A VIEW FROM THE BENCH: JUDICIAL PERSPECTIVES ON DIGITAL EVIDENCE Honorable Ronald J. Hedges Honorable Joseph A. Grasso Jr. Honorable Gregory I. Massing Honorable Janet L. Sanders
108	Bitcoin & Electronic Currency	
111	Cellebrite Demonstration	
112	The Power of Plaso for Smartphone and Computer Forensics	
113	Gleaning Artifacts from Network Packet Capture (PCAP) Files	
115	Twitter Investigations	
116	MDEC - Report Writing and Testimony	
117	How Machine Learning is Facilitating Video Management and Public Records Requests	
201		
202	Collection of Digital Evidence – Without Search Warrant	

NETWORKING SESSION - HOSTED BY MDEC

EXHIBITOR HALL - 5:30 PM - 7:00 PM

Session 3 | 2:30 PM: 3:45 PM
Descriptions

Wireless Technologies
Room: 101 | **Type**: Lecture

This session will provide a broad overview of wireless communication technologies, including satellite, cell phone, and IEEE 802 networks. IEEE 802.11 Wi-Fi networks, the relationship between levels of network addressing (e.g., MAC, IP, SSID, and BSSID), and ways to detect stations on a Wi-Fi network will be discussed.

Instructor: Dr. Gary Kessler

Sextortion: Findings from NCMEC's Cyber Tipline
Room: 102 | **Type**: Lecture

Join NCMEC for a look at the findings from an in-depth analysis of sextortion reports from the NCMEC CyberTipline.To better understand the "who, what, where, when & why" of sextortion, NCMEC analyzed reports that were made to the CyberTipline over 18-months.Findings from this analysis will highlight child age and gender differences regarding the patterns and manipulation tactics used in cases of sextortion. The implications of these findings will also be discussed.

Instructor: Rebecca Sternburg

Bridging the Gap Between Computer and Mobile Device Forensic Examinations
Room: 103 | **Type**: Lecture

Crimes involving digital evidence are increasingly focused on mobile devices, usually examined by separate tools from those used for computers. Nuix solves this disconnect with our ability to analyze mobile evidence alongside other, traditional forms of computer and human-generated data. Using visualization, timeline analysis and advanced filtering and searching capabilities, Nuix can help streamline the review process and efficiently get to the relevant items of interest to the investigator.

Instructor: Tim Moniot

Survey of Gaming in Massachusetts - Casinos, Fantasy Sports and Sportsbetting
Room: 104 | **Type**: Lecture

This course focuses on gaming in Massachusetts -- including legalized casino gaming, regulated online daily fantasy sports and illegal gaming (sportsbetting, unlicensed slots, lotteries) -- and the intersection with cyber crime. The challenges faced here are faced in many jurisdictions, so this course will be applicable beyond Massachusetts.

Instructor: Patrick Hanley

Session 3 | 2:30 PM: 3:45 PM
Descriptions

ECPA/SCA
Room: 105/106 | **Type**: Lecture

If you learn that your suspect has used a social network provider, electronic mail service, cloud backup, or cellular service to commit a crime, do you know how to respond? Have you heard of the Federal Electronic Communications Privacy Act? What about the Stored Communications Act? Are you aware of search warrant statutes that deal specifically with the collection of digital evidence from these types of providers? If you don't, you should, because odds are you will have to collect this type of evidence in the near future. The legal requirements can be confusing. Attendees to this session will learn the proper way to demand records from electronic communication service providers in the legally appropriate manner.

Instructor: Abigail Abraham

Overcome Your Toughest Forensic Challenges with Cellebrite Advanced Investigative Services
Room: 107 | **Type**: Lab

Backed by the leading team of forensic researchers in the industry, combined with strategic relationships with top service providers, Cellebrite continues to deliver breakthrough solutions to the law enforcement community to liberate data from locked, encrypted, and damaged mobile devices. Come join Dan Embury, Technical Director of Cellebrite Advanced Investigative Services (CAIS) and Rene Novoa, Senior Manager of Forensics eDiscovery at DriveSavers, for an enlightening discussion on the latest techniques and solutions to overcome your toughest challenges.

Instructor: Dan Embury | Rene Novoa

Bitcoin and Electronic Currency
Room: 108 | **Type**: Lab

Attendees will be exposed to the concepts of crypto-currency and their use in crimes. Also, discussed will be the concepts of investigating crypto-currency by law enforcement.

Instructor: Todd Shipley

The Power of Plaso for Smartphone and Computer Forensics
Room: 112 | **Type**: Lecture

Plaso is a powerful open source forensic framework developed by Google, with collaboration from multiple organizations involved in cutting-edge digital forensics. This enhanced framework can extract forensic artifacts from Windows, Mac OS, Linux, Windows Phone, iOS, and Android OS. Furthermore, Plaso has a plugin architecture that allows practitioners to add new capabilities, such as parsing data from smartphone applications that are not supported by commercial forensic tools. Plaso also provides a mechanism to load all extracted data into a consolidated database for correlation, searching, and analysis. This session demonstrates the capabilities of Plaso and introduces plugin development concepts.

Instructor: Dr. Eoghan Casey

Session 3 | 2:30 PM: 3:45 PM
Descriptions

Gleaning Artifacts from Network Packet Capture (PCAP) files
Room: 113 | **Type**: Lab

In this hands-on lab, students will use Wireshark and Network Miner to collect artifacts of importance from packet capture files (network traffic). This is an important skill when investigating any computer network related cases. Students will data mine network traffic for graphic files, screen names, and keywords. Instructed by experienced investigators. Adapted from NW3C's Cybersecurity 235 - Basic Network Intrusion Investigations http://www.nw3c.org/training/Computer-Crime/126

Instructors: Cynthia Gonnella | Michael Stern

Twitter Investigations
Room: 115 | **Type**: Lab

Twitter has quickly become the go-to medium for today's instant communication, proven by the fact that there are 5000 tweets per second. Twitter searching will be introduced to allow searching for Twitter profiles, tweet keywords and hashtags, and even searching for tweets from a particular latitude and longitude. These Twitter searching techniques will include both standard and hidden Boolean operators, ensuring that investigators have access to the best possible evidence.

Instructors: Lauren Wagner | Dean Chatfield

MDEC (Module 2) (Report Writing)
Room: 116 | **Type**: Cert |

This cert is a continuation from Sessions 1 and . Pre-registration is required for admittance into this cert.

Instructor: Massachusetts Digital Evidence Consortium

How Machine Learning is Facilitating Video Management and Public Records Requests
Room: 117 | Lecture

Video in law enforcement has become a powerful tool in how agencies protect themselves, as well as private citizens. Challenges exist however, in how agencies effectively manage all of this of this video - Curating thousands of hours of video can be a costly and resource intensive process. Agencies are looking to new technologies to help them automate their video management processes: Extracting spoken content, image stabilization, object recognition, redacting (blurring), sentiment and motion detection. In this session, learn how agencies are addressing these and other challenges by leveraging new Cloud based machine learning technologies, that offer advanced video analytics and management capabilities.

Instructor: Jeff King | John Newsom

Collection of Digital Evidence – Without Search Warrant
Room: 202 | **Type**: Cert

This presentation explores the different types of search and seizure used in technology--facilitated child sexual exploitation (TFCSE) cases. The audience learns the differences between a consent search and a search warrant, and discusses applicable cases for each.

Instructor: Margaret M. Ogarek

A View from the Bench: Judicial Perspectives on Digital Evidence

4:00 PM - 5:30 PM | Tiffany Ballroom

Digital evidence is present in nearly every criminal case. Often, the digital evidence issues in these cases involve a complex evaluation of the intersection of law and technology. This panel discussion will provide the judicial perspective on digital evidence and cyber crime.

Topics will include the 4th Amendment and digital evidence; whether we should treat digital evidence searches differently than home searches; search protocols for digital evidence; and the plain view doctrine in digital evidence searches.

Honorable Ronald J. Hedges
Magistrate Judge in the United States District Court for the District of sNew Jersey (ret.)

Honorable Joseph A. Grasso Jr.
Associate Justice of the Massachusetts Appeals Court (ret.)

Honorable Gregory I. Massing
Associate Justice of the Massachusetts Appeals Court

Honorable Janet L. Sanders
Justice of the Massachusetts Superior Court

Day 2 Morning Agenda

Lecture | Lab | Cert | Prosecutor 3 Day

Conference Info

Featured Speakers

Day 1 Morning Sessions 1 and 2

Day 1 Afternoon Session 3 & Judicial Panel

Day 2 Morning Sessions 4, 5, and 6

Room	SESSION 4 8:30 AM - 9:40 AM	SESSION 5 9:50 AM - 11:00 AM	SESSION 6 11:10 AM - 12:20 PM
101	Digital Forensic Report Writing		Tracing IP Addresses
102	Harnessing Digital Data to Accelerate Criminal Investigations through Actionable Insights	Preparing to Testify About Mobile Evidence in Court	Leveraging Data From Social Media and the Cloud to Accelerate Investigations
103	Swatting, Doxing and PEDs: Investigative Strategies & Best Practices	Technology in Policing - 2016 and Beyond	
104	A Multidisciplinary Approach to Human Trafficking Investigations	Understanding Victims: Identifying Trafficked & Commercially Sexually Exploited Children	Online Human Trafficking Investigations
105/6	Social Media Panel	Working with Yahoo During an Investigation	Facebook
107	PowerPoint 101	PowerPoint 102	ICAC Tools for ICAC Investigators
108	Deep and Dark Web Investigations	Autopsy 4.0	
111	XRY Demonstration	Nuix Demonstration	DriveSavers Demonstration
112	Windows Forensic Environment (WinFE)	Extracting Cloud Data Using Tokens Obtained From Cell Phones	Cell Phone Forensics
113	Volatile Data Collection (Local Machine & Network)	Windows Virtual Machines for Use in Computer and Network Forensics	Processing Windows Event Logs for Timelining Criminal Cases
115	SEARCH Investigative Resources	Undercover Investigations	
116	MDEC Search and Seizure		
117	How Machine Learning is Facilitating Video Management and Public Records Requests	Microsoft Online, Safety & Services Overview	Community on Patrol: Citizens as Sensors to Fight Terrorism, Reduce Crime, & Improve Public Safety
201	Assessing a CCTV DVR in the Field	Recovery of Video Evidence Using DVR Examiner	Forensic Audio Clarification Basics
202	Experts, Evidence, and Multimedia Exhibits	Submitting Mobile Device Evidence into Court – What Can You Recover?	Submitting Mobile Device Evidence into Court – What Can You Get From Mobile Providers

LUNCH - FEATURED SPEAKER
Jim Emerson, IACP
TIFFANY BALLROOM - 12:30 PM - 1:45 PM

Session 4 | 8:30 AM: 9:40 AM
Descriptions

Digital Forensics Report Writing
Room: 101 | **Type**: Lecture

This session will describe the elements of a digital forensics report, including the different items of information, with a rationale for each section. Discussion will also show how an examiner's report might integrate the reports generated by forensics tools. The importance of identifying and writing to your audience will also be discussed, as well as the place for opinions. Finally, we will discuss some topics that are known to be particularly confusing to many non-technical readers.

This session continues in Session 5.

Instructor: Dr. Gary Kessler

Harnessing Digital Data to Accelerate Criminal Investigations through Actionable Insights
Room: 102 | **Type**: Lecture

In this interactive session, attendees will experience first-hand how digital forensics technology can accelerate an entire investigative process to help investigators unlock critical evidence to break cases faster. Using a drug/gang investigative scenario, investigators and prosecutors will learn how emerging digital forensics analytics, data management capabilities, tiering strategies, and secure workflows can change the way they can access, analyze, and act on critical data at different points in an investigation. The workshop will address key digital evidence trends that IACP and others have identified, such as the increased reliance on evidence from Cloud and Social Media accounts and the emerging interest in making data from digital sources available to investigators, first responders and prosecutors to support the public safety mission.

In this session, attendees will learn how to:

- Transform digital data into evidence that a non-technical investigator can use quickly and intuitively.
- Leverage data from Private Social Media and Cloud accounts much earlier in an investigation.
- Deploy secure, collaborative investigative workflows that extend digital data extraction, delivery and analysis capabilities to the right people at the right time while supporting chain of custody requirements and standard operating procedure.
- Develop an agency-wide digital forensics architecture that makes extraction and analysis capabilities available to investigators, first responders, examiners, and prosecutors while preserving the integrity of evidence.

Instructor: Rich Colangelo | Brendan Morgan

Swatting, Doxing and PEDs: Investigative Strategies & Best Practices
Room: 103 | **Type**: Lecture

This course provides an overview of swatting and doxing. Attendees will also be exposed to investigative strategies pertaining to real-time swatting incidents, steps one can take to minimize their internet footprint and best practices for seizing/handling portable electronic devices (PEDs).

Instructor: Detective Sergeant David Costantino

Session 4 | 8:30 AM: 9:40 AM
Descriptions

A Multidisciplinary Approach to Human Trafficking Investigations
Room: 104 | **Type**: Lecture

This course will review the Human Trafficking statute in Massachusetts and provide information on the multidisciplinary approach of the Attorney General's Office.

Instructor: Deborah Bercovitch | Nikki Antonucci | Detective Sergeant Mary McCauley

Social Media Panel
Room: 105/6 | **Type**: Lecture

This panel will feature representatives from various social media companies, and will provide an opportunity for representatives to explain their law enforcement policies on issues such as user notification, cybertips, meeting particularity requirements of the 4th Amendment, how to best get in touch with a live law enforcement liaison, as well as how to get questions answered that are not covered in law enforcement guidelines. Audience members will be able to ask questions and interact with social media representatives.

Panelists: Abigal Abraham | Andrea Kirkpatrick | Acadia Senese | Chris Madsen | Tracy Ingle

PowerPoint 101
Room: 107 | **Type**: Lab

Learn how to use PowerPoint. If you are new to Microsoft PowerPoint, you will find all the basics you need to know right here, to create effective and professional looking presentations for court, community presentations or department/agency trainings & briefings.

In this PowerPoint 101 course you will learn the basic concepts of creating and editing simple, effective PowerPoint presentations. This course consists of lecture and lab where you will gain hands on knowledge of one of the most popular presentation tools in use today. When you are done, you will be able to skillfully present your message in the courtroom, squad room or in the community meeting room.

You will begin by exploring explore unique features found in PowerPoint like "The Microsoft Ribbon" and contextual tabs. A tour of PowerPoint menus will lead to the creation of basic slide layouts. You will learn how to add text boxes and use style & formatting to turn your presentation into a polished, professional tool to convey your topic to your audience.

You will be shown how to use simple animations and transitions to add emphasis and sophistication to your message. You will see how simple and straight-forward methods of inserting photos, audio and video can bring your presentation to life! Discussion will also include the "Do's & Don'ts of PowerPoint" and how to avoid "Death by PowerPoint".

Instructor: Paul Melaragni

Session 4 | 8:30 AM: 9:40 AM
Descriptions

Deep and Dark Web Investigation
Room: 108 | **Type**: Lab

The course discusses Deep and Dark Web investigations. It focuses on differences between Deep and Dark Web and how cybercriminals use Deep and Dark Web. Additionally, this course involves profile discussions of Deep Web forums, Dark Web forums, IRC chatrooms, Jabber (XMPP) chats, Pastebin leaks, and marketplaces. It involves a live demonstration on how to build a threat actor profile

Instructors: Vitali Kremez | Luke Rodeheffer

Previewing with WinFE in a lab environment
Room: 112 | **Type**: Lab

In recent years Windows Forensic Environment (WinFE) has become the standard for many law enforcement personnel who have a need to preview computers in a forensically sound manner. During this block we will explore the use of WinFE as a preview tool in a lab environment; however, we will also discuss its use for on-site preview. In addition to previewing, we will look at using WinFE to access some newer laptops and tablets, many of which now come configured 'UEFI Only' with no legacy support.

Instructor: John Riley

Volatile Data Collection - Local Machine and Network
Room: 113 | **Type**: Lab

In this hands-on lab, students will learn to use ProDiscover-IR to collect important system information and volatile artifacts from a live machine both locally and remotely over a network. Instructed by experienced investigators.This block was adapted from NW3C's Cybersecurity 235 - Basic Network Intrusion Investigations course http://www.nw3c.org/training/Computer-Crime/126

Instructors: Cynthia Gonnella | Michael Stern

SEARCH Investigative Resources
Room: 115 | **Type**: Lab

SEARCH has offered technology-driven solutions to the law enforcement community for over 40 years. This session will explore the cutting edge services and products SEARCH uses to aid investigators in crimes with digital evidence. These resources also provide guidance on utilizing technology to corroborate evidence in traditional crimes. Topics include the new SEARCH add-on (a replacement for the SEARCH Investigative Toolbar), available for Firefox, Chrome, and Safari; The SEARCH Electronic Service Provider (ESP) List to find legal contacts for investigative purposes; technology guides that cover current investigative trends; and our online video presentation series, eLearning offerings and podcast series.

Instructors: Lauren Wagner | Dean Chatfield

Session 4 | 8:30 AM: 9:40 AM
Descriptions

MDEC Digital Evidence Handler Certification Training
Room: 116 | **Type**: Cert

This five-session module will review the collection and control of digital evidence. Each attendee will need to complete an exam that will be graded towards the Digital Evidence Certification Program. This certification continues through session 5, 6, 7 and 8.

Instructor: Kevin Connolly

How Machine Learning is Facilitating Video Management and Public Records Requests
Room: 117 | Lecture

Video in law enforcement has become a powerful tool in how agencies protect themselves, as well as private citizens. Challenges exist however, in how agencies effectively manage all of this of this video - Curating thousands of hours of video can be a costly and resource intensive process. Agencies are looking to new technologies to help them automate their video management processes: Extracting spoken content, image stabilization, object recognition, redacting (blurring), sentiment and motion detection. In this session, learn how agencies are addressing these and other challenges by leveraging new Cloud based machine learning technologies, that offer advanced video analytics and management capabilities.

Instructor: Jeff King | John Newsom

Assessing a CCTV DVR in the Field
Room: 201 | **Type**: Lecture

Arriving on scene and finding a digital video recorder doesn't have to be a stressful process. While it isn't always as easy as the old days of ejecting a VHS tape from the recorder, there are several ways to recover video evidence at the scene. In this session, we'll discuss the pros and cons of several of these methods, as well as provide some insight into when and where to use each.

Instructors: Jimmy Schroering

Experts, Evidence, and Multimedia Exhibits
Room: 202 | **Type**: Cert

This course will feature a Multimedia Director and Assistant District Attorney as they work together to create multimedia exhibits for trial. This presentation shows attendees how to utilize free software in developing visuals for display throughout a trial and in deliberation.

Instructors: Assistant District Attorney Anne Yas | Colleen Crawford

Session 5 | 9:50 AM: 11:00 AM
Descriptions

Digital Forensics Report Writing
Room: 101 | **Type**: Lecture

This session is a continuation from Session 4.

Instructor: Dr. Gary Kessler

Preparing to Testify About Mobile Evidence in Court
Room: 102 | **Type**: Lecture

Being prepared to take a judge and jury through your investigative process, and why mobile evidence is relevant to your case, is only part of providing persuasive testimony. You should also be prepared to testify about the tools and methods you used, and to address any challenges to your process that might be raised by the defense. This session will tell you what you need to know about mobile forensic extraction, analysis, interpretation and validity of findings; how to deal with questions about vendors' proprietary methods; and specific challenges around mobile evidence authenticity and admissibility. In addition, attendees will learn best practices for compiling formal reports that catalogue evidence for presentation in court and how to properly document evidence using a series of sample reports. Rich Colangelo, and Brendan Morgan will guide attendees with a unique blend of insights that combine the perspectives of a seasoned prosecutor and forensic examiner with decades of shared experience.

Instructor: Rich Colangelo | Brendan Morgan

Technology in Policing - 2016 and Beyond
Room: 103 | **Type**: Lecture

Law enforcement must understand the latest technical advances to conduct criminal investigations. But cyber components of criminal investigations are only one way technology is shaping modern policing. Investigators today use technology as investigative and intelligence tools. And law enforcement agencies and police officers are the frequent target of cyber attacks. Hear a panel of experts discuss the current and future use of technology in criminal investigations and intelligence as well as emerging cyber threats to police and law enforcement agencies. Learn how to use technology as a weapon in your investigative arsenal, and interact with our panelists to uncover new resources that will enhance your investigations upon return.

This panel continues in Session 6.

Panelists: John Daley | Scott Range | Kevin Swindon | Jim Emerson

Understanding Victims: Identifying Trafficked and Commercially Sexually Exploited Children
Room: 104 | **Type**: Lecture

My Life My Choice is a national leader in prevention and intervention around the Commercial Sexual Exploitation of Children (CSEC). They train youth service providers on how to understand, recognize, and intervene on behalf of girls and boys experiencing the trauma of sexual exploitation. The Understanding Victims Training gives the audience a clear definition of what constitutes CSEC, how girls and boys become exploited, and how to identify victims and help them find a path to safety.

Instructor: Audrey Morrissey

Session 5 | 9:50 AM: 11:00 AM
Descriptions

Working with Yahoo During an Investigation
Room: 105/6 | **Type**: Lecture

This presentation will provide an overview of Yahoo services, describe the types of data available to law enforcement from those services, and review Yahoo process and policy for providing data to law enforcement, consistent with state and federal law, including the Stored Communications Act. In addition, we will review some best practices compiled by Yahoo's Law Enforcement Response Team, the folks responding to law enforcement requests for data.

Instructor: Chris Madsen

PowerPoint 102
Room: 107 | **Type**: Lab

In this PowerPoint 102+ course, you will learn technical concepts that can be applied to the development of numerous interactive courtroom exhibits. You will be given the tools to transform, otherwise static exhibits, into interactive, animated, multimedia exhibits, empowering you to present the facts of a case in the most compelling way.

You will learn how to combined audio and with transcripts, generating synchronized text overlays on a 911 call. You will also learn how to build interactive DNA charts, an interactive timeline, an interactive anatomy diagram that displays multiple points of trauma, animated chalks and much more.

You will be shown how to utilize additional software to generate layers of multimedia into your PowerPoint courtroom presentation/closing argument. This course will not only streamline your workflow, but also clarify large amounts of data and strengthening your impact on a jury.

Instructor: Coleen Crawford

Autopsy 4: The Most Powerful Digital Forensics Platform You'll Find for Free
Room: 108 | **Type**: Lab

Autopsy 4 is an open source, collaborative, end-to-end digital forensics platform. With an easy-to-use interface and all the standard features -- file recovery, keyword search, hash matching, registry analysis, etc. -- that digital forensic examiners need and expect from commercial digital forensics tools, it also offers unique analytical features including image and timeline analysis. This hands-on workshop covers these and other exciting features including brand-new collaborative functions.

This lab continues in Session 6.

Instructor: Dr. Brian Carrier

Session 5 | 9:50 AM: 11:00 AM
Descriptions

Extracting Cloud Data Using Tokens Obtained from Cell Phones
Room: 112 | **Type**: Lab

Learn how to recover cloud data from mobile devices using the tokens or credentials collected during cell phone dumps.

Instructors: Rey Navarro

Windows Virtual Machines for Use in Computer and Network Forensics
Room: 113 | **Type**: Lab |

In this hands-on lab, students will simulate the creation of a Windows virtual machine using Windows built-in Hypervisor technology, and work with a pre-built Hypervisor VM. This is an important skill for forensic examiners, as it allows them to work a case while maintaining control of contraband at all times and protects their underlying forensic machine from malware. Instructed by experienced investigators. Adapted from NW3C's Cybersecurity 235 - Basic Network Intrusion Investigations course.

Instructors: Cynthia Gonnella | Michael Stern

Undercover Investigations
Room: 115 | **Type**: Lab

When law enforcement officers conduct online investigations, there are operational security best practices to consider. This course will provide an overview of configuring and deploying managed attribution Internet systems, tips for managing multiple online accounts, alias tradecraft, and legal considerations. Participants will also receive a "cheat sheet" highlighting ways to protect their online digital footprint.

Instructor: Tom Doyle

MDEC Digital Evidence Handler Certification Training
Room: 116 | **Type**: Lecture

This is a continuation from Session 4 and continues in Sessions 6, 7, and 8.

Instructor: Kevin Connolly

Microsoft Online, Safety & Services Overview
Room: 117 | **Type**: Lecture

This presentation will provide an overview of the major online services which Microsoft provides to customers including Outlook.com (Hotmail), OneDrive, Skype and XBox. For each service, you will learn what data may be available with the appropriate service of legal process, where and how to serve legal process, user notification policies, requirements for threat-to-life emergency requests, and response expectations.

Instructors: Tracy Ingle

Session 5 | 9:50 AM: 11:00 AM
Descriptions

Recovery of Video Evidence Using DVR Examiner
Room: 201 | **Type**: Lecture

Recovering video evidence from CCTV digital video recorders (DVRs) can be a difficult process, but it doesn't have to be. DVR Examiner is a software solution for acquiring video and metadata from CCTV DVRs in a forensically sound manner. In this session, we will demonstrate how to recover evidence quickly and easily from a DVR hard drive or forensic image. We will also briefly discuss the technical processes behind DVR Examiner.

Instructors: Jimmy Schroering

Submitting Mobile Device Evidence into Court – What Can You Recover?
Room: 202 | **Type**: Cert

This presentation examines the role of mobile devices in criminal activities. Participants will learn mobile devices store information and the different type of extractions to recover evidence from mobile devices. The different types of evidence recoverable from mobile devices will be discussed. Participants will be shown different examples of software and hardware commonly used to conduct cell phone extractions.

Instructor: Justin Fitzsimmons | Lauren Wagner

Session 6 | 11:10 AM: 12:20 PM
Descriptions

Tracing IP Addresses
Room: 101 | **Type**: Lecture

This session will describe how to trace IP addresses and other source data on the Internet. Topics include Internet Protocol (IP) addresses and Internet domains, determining address/domain name ownership, and, most importantly, who pays for a domain name. The structure of the Internet, anonymizers, packet tracing, geolocation, and higher-layer protocol issues will also be discussed.

Instructor: Dr. Gary Kessler

Leveraging data From Social Media and the Cloud to Accelerate Investigations
Room: 102 | **Type**: Lecture

With 71% of people using their mobile devices to access social media, the need to access this data during criminal investigations has become imperative. In this interactive session, we will provide an update on the emerging opportunity to legally obtain digital evidence from private social media and cloud sources. The program will review the relevance of cloud data to investigations, the types of information that can be uncovered, best practices for collecting and managing evidence, legal considerations and due process, and sample warrant templates. The session will review case studies from agencies that have adopted cloud extraction technology to reduce the cycle times associated with waiting for service providers to fulfill request. We'll also show how data from cloud and social media accounts can "complete the puzzle" in investigations by complementing information obtained from the device itself. Finally, we will share recommendations for incorporating this technology into a forensic operation by developing standard operating procedure and training.

Instructor: Ronan Engler | Rene Novoa

Technology in Policing - 2016 and Beyond
Room: 103 | **Type**: Lecture

This panel is a continuation from Session 5.

Panelists: John Daley | Scott Range | Kevin Swindon | Jim Emerson

Online Investigations of Human Trafficking
Room: 104 | **Type**: Lecture

Attendees will learn about the current issues of Internet Investigations. How to safely get online, properly document an investigations and find your target on social media and other sites.

Instructor: Todd Shipley

Facebook
Room: 105/6 | **Type**: Lecture

In this course, Andrea will discuss the Facebook "basics", the latest safety and privacy controls available to prevent and reduce risks for users of the site, safety initiatives designed to combat crimes, and a detailed review of Facebook's on-line records request system for law enforcement use.

Instructor: Andrea Kirkpatrick

Session 6 | 11:10 AM: 12:20 PM
Descriptions

ICAC Tools for ICAC Investigations
Room: 107 | **Type**: Lab

This lab is aimed at those individuals who are new to investigating online child exploitation cases. Covered in this class will be the set up and configuration of a host of tools recommended for conducting online undercover investigations. The tools that will be discussed include Chrome browser with Google Drive, Exif Scrubber, Exif editor, Opanda, Fireshot, and Google Image search.

Instructor: Jeffrey Rich

Autopsy 4: The Most Powerful Digital Forensics Platform You'll Find for Free
Room: 108 | **Type**: Lab

This lab is a continuation from Session 5.

Instructor: Dr. Brian Carrier

Cell Phone Forensics
Room: 112 | **Type**: Lab

Learn about techniques used to examine popular smartphones, specifically iOS- and Android- based devices, including methods used to bypass / recover security codes and swipe patterns. Attendees will learn how to recover vital chat data from messaging apps and correlate common data between multiple devices via instantly plotted connection diagrams, timelines, and geomaps.

Instructors: Wil Hernandez

Processing Windows Event Logs for Timelining Criminal Cases
Room: 113 | **Type**: Lab

In this hands-on lab, students will use Fire-Eye Mandiant's Redline to collect and process data to tell a story of how files came to be on a particular machine. This skill is very important when working computer facilitated criminal cases. Students learn to timeline Internet history, file downloads, program installations, programs run, files accessed, and by what account. Instructed by experienced investigators. Adapted from NW3C's Cybersecurty 235 - Basic Network Intrusion Investgations course.

Instructors: Cynthia Gonnella | Michael Stern

Developing an Undercover Online Profile
Room: 115 | **Type**: Lab

This lab is a continuation from Session 5.

Instructor: Tom Doyle

MDEC Digital Evidence Handler Certification Training
Room: 116 | **Type**: Cert

This is a continuation from Sessions 4 and 5 and continues in Sessions 7 and 8. Attendees may participate as "members of the jury or public."

Instructor: Kevin Connolly

Session 6 | 11:10 AM: 12:20 PM
Descriptions

Community on Patrol: Citizens as Sensors to Fight Terrorism, Reduce Crime, and Improve Public Safety

Room: 117 | **Type**: Lecture

With recent terrorist attacks, law enforcement agencies are investing in new sensor based technologies (surveillance systems, drones, etc.) and location-based data feeds to gather intelligence and respond proactively to public safety concerns. One challenge faced however, is how to tap into the vast amount of data being generated by private citizens. Videos, photos, and social media posts, created using smartphones, have the potential to provide first responders with information that could aid in their efforts. In this session, hear how the Miami-Dade police department has developed a new smartphone application Community On patrol, designed to deputize the counties 2.6 million residents and improve community relations.

Instructors: Jeff King

Forensic Audio Clarification Basics

Room: 201 | **Type**: Lab

Often times subject interviews, 911 calls, and informant recordings, are un-intelligible and difficult to hear. Through forensic audio clarification, there are many different kinds of processes that can be performed to make these recordings easier to understand. In this session, examples will be provided of what can (and cannot) be done when it comes to clarification.

Instructors: Brewster Rolland-Keith

Submitting Mobile Device Evidence into Court – What Can You Get From Mobile Providers

Room: 202 | **Type**: Cert |

This presentation will cover the various methods of introducing the results of cell phone extractions into evidence in court. Issues of Daubert challenges to the introduction and responses to Daubert challenges will be examined. The role of Motions in Limine will also be discussed.

Instructor: Justin Fitzsimmons | Lauren Wagner

Day 2 Afternoon Agenda

Lecture | Lab | Cert | Prosecutor 3 Day

Day 2 Afternoon Sessions 7 and 8

Day 3 Morning Sessions 9, 10 and 11

Day 3 Afternoon Sessions 12 and 13

Bios

Sponsors/Exhibitors

Room	SESSION 7 2:15 PM - 3:30 PM	SESSION 8 3:45 PM - 5:00 PM
101	Popular Scams and Exploits	Mobile Device Forensics
102	Finding the Needle in a Haystack: Enhancing Insights Through Unified Investigative Workflows	Overcoming Persistent Smartphone Forensics Challenges
103	Middle East Terrorism and the Challenge's for Modern Societies	
104	Sex Trafficking & the Commercial Sexual Exploitation of Children	
105/6	Experts, Evidence, and Multimedia Exhibits	Google
107	PALADIN	RECON
108	Autopsy 4.0	
111	Paraben Corporation Demonstration	
112	Salvaging Difficult to get Digital Evidence Using Advanced Carving Methods	Windows Forensic Environment (WinFE)
113	Gleaning Artifacts from Network Packet Capture (PCAP) Files	Volatile Data Collection (Local Machine & Network)
115	Searching Facebook and Instagram	
116	MDEC Search and Seizure	
117	Technical Support Scams: Investigating and Preventing Tech Scams	Microsoft and TASER Leverage the Cloud to Drive Safer Communities
201	Presenting Audio/Video Evidence in Court	
202	Submitting Mobile Device Evidence into Court – Encryption Issues	Collection of Digital Evidence – ECPA

NETWORKING SESSION - HOSTED BY CELLEBRITE

Outdoor Pavilion - 5:00 PM - 7:00 PM

Session 7 | 2:15 PM: 3:30 PM
Descriptions

Popular Scams and Exploits
Room: 101 | **Type**: Lecture

This course covers the more disturbing and popular scams and cons occurring via the internet and high technology. The techniques to identify the bad guys and artifacts the scams leave behind will be shown and discussed.

Instructors: Michael Menz | Detective Kipp Loving

Finding the Needle in a Haystack: Enhancing Insights Through Unified Investigative Workflows
Room: 102 | **Type**: Lecture |

When a crime occurs, the race to generate leads, identify suspects and make arrests begins. With mobile data sources and case backlogs growing in volume and complexity – and many cases now involving multiple devices -- forensic examiners, analysts, investigators, and prosecutors require new purpose-built analytics capabilities to quickly view, sort, analyze and cross reference large sets of mobile and private cloud data to provide the context that allows them work cases faster and keep their communities safe. This session will present strategies and techniques for enabling intuitive analysis by everyone on an investigative team. Attendees will learn the benefits of breaking down silos of digital information using a unified investigative model that unlocks the intelligence of mobile and digital evidence. We will also show how the ability to and correlate and cross-reference data sets using sophisticated image, video, and text analytics can reveal leads, insights and patterns faster, enabling users across multiple locations to efficiently search, share, and report on mobile and digital forensic evidence.

Instructor: Ronan Engler | Rene Novoa

Middle East Terrorism and the Challenge's for Modern Societies
Room: 103 | **Type**: Lecture

This session is focused on terrorism in the USA, Middle East, Europe, East & West Ideologies, the effect on society, and responding challenges facing the United States & Europe.

Instructors: Majid Hassan

Sex Trafficking & the Commercial Sexual Exploitation of Children
Room: 104 | **Type**: Cert

Attendees will learn the basics about human sex trafficking and the commercial sexual exploitation of children. Content includes misconceptions of human trafficking, venues for commercial sex work, domestic versus international trafficking, demand for sex, victimization involving commercial sex work, vulnerable populations and how vulnerabilities are exploited, organization of a trafficking enterprise, who the traffickers are, how traffickers/pimps control their victims and methods to identify

Instructor: Sergeant Daniel Steele

Session 7 | 2:15 PM: 3:30 PM
Descriptions

Experts, Evidence, and Multimedia Exhibits
Room: 105/6 | **Type**: Lecture

This course will feature a Multimedia Director and Assistant District Attorney as they work together to create multimedia exhibits for trial. This presentation shows attendees how to utilize free software in developing visuals for display throughout a trial and in deliberation.

Instructors: Assistant District Attorney Anne Yas | Colleen Crawford

PALADIN
Room: 107 | **Type**: Lab

PALADIN has become the World's #1 Forensic Suite used by thousands of digital forensic examiners from Law Enforcement, Military, Federal, State and Corporate agencies. The PALADIN Toolbox combines the power of several court-tested Open Source forensic tools into a simple interface that can be used by anyone. With the PALADIN Toolbox a user can easily and quickly TRIAGE – SEARCH – IMAGE and more! Join the SUMURI Team as we lead participants through a cadre of some of the most open source tools compiled on SUMURI'S PALADIN Forensic Suite. Learn what is available for conducting professional investigations and analysis using freely available tools.

Instructor: Manny Kressel

Autopsy 4: The Most Powerful Digital Forensics Platform You'll Find for Free
Room: 108 | **Type**: Lab

Autopsy 4 is an open source, collaborative, end-to-end digital forensics platform. With an easy-to-use interface and all the standard features -- file recovery, keyword search, hash matching, registry analysis, etc. -- that digital forensic examiners need and expect from commercial digital forensics tools, it also offers unique analytical features including image and timeline analysis. This hands-on workshop covers these and other exciting features including brand-new collaborative functions. This lab continues in Session 8.

Instructor: Dr. Brian Carrier

Salvaging Difficult to get Digital Evidence Using Advanced Carving Methods
Room: 112 | **Type**: Lecture

File carving enables digital investigators to recover deleted information from digital media and devices that offenders thought was irretrievable. In addition, carving methods are also useful for extracting useful information from sources that are more challenging to deal with, including memory dumps, network streams, and partial or corrupt files or disk images. As the capacity of digital media grows and offenders increasingly delete incriminating digital evidence, there is a growing need to recover deleted and dense data from digital devices in a timely manner. Existing tools take a long time to run and produce a large number of junk files that require human review. Recent advances in file carving have developed ways to accelerate the process, piece together non-contiguous file fragments, and reduce the number of junk files. This session demonstrates advanced methods and tools for salvaging deleted files for forensic purposes, including fragmented and partial videos. Strengths and weaknesses of different file carving methods are presented.

Instructor: Dr. Eoghan Casey

Session 7 | 2:15 PM: 3:30 PM
Descriptions

Gleaning Artifacts from Network Packet Capture (PCAP) files

Room: 113 | **Type**: Lab

In this hands-on lab, students will use Wireshark and Network Miner to collect artifacts of importance from packet capture files (network traffic). This is an important skill when investigating any computer network related cases. Students will data mine network traffic for graphic files, screen names, and keywords. Instructed by experienced investigators. Adapted from NW3C's Cybersecurity 235 - Basic Network Intrusion Investigations http://www.nw3c.org/training/Computer-Crime/126

Instructors: Cynthia Gonnella | Michael Stern

Searching Facebook and Instagram

Room: 115 | **Type**: Lab

Facebook is the largest worldwide social media website and contains a substantial amount of potential investigative information. Facebook information can be searched in three separate and distinct ways. One method is to use Facebook graph search, which uses specific targeted terms that, when used correctly, can show investigative material. The instructor will demonstrate how graph search works, and explain how syntax—the structure of the search keywords and phrases—is vital to a successful search. The second method is to use URL manipulations. Once a Facebook profile has been identified, these URL manipulations can show content from this target, such as photo comments, video likes, and comparisons with friends. These URL manipulations are specific and offer information beyond what can be found simply by looking at someone's profile. The third method uses Google advanced and Boolean operators to search on Facebook in a more broad sense. Constructing a good keyword string is key to ensuring that investigative material is found. The instructor will demonstrate examples of specific syntax that should be used. Additionally, searcing techniques for Instagram will be addressed, including searching by name, username, keyword, and even geographical area.

This session continues in Session 8.

Instructors: Lauren Wagner | Dean Chatfield

MDEC Digital Evidence Handler Certification Training

Room: 116 | **Type**: Lecture

This is a continuation from Sessions 4, 5, and 6 and continues in Session 8.

Instructor: Kevin Connolly

Session 7 | 2:15 PM: 3:30 PM
Descriptions

Technical Support Scams- Investigating and Preventing Tech Scams
Room: 117 | **Type**: Lecture

This panel discussion will cover the scope of the tech support scam problem faced by law enforcement today, currently estimated as affecting 3.3 million consumers each year with an average financial loss of $454 per consumer, or $1.5 billion. Part two will be devoted to identifying practical investigative approaches and available resources to hold tech scammers accountable for their illegal acts, including:

(a) resources for identification of victims,
(b) forming multi-jurisdictional investigative teams v. individual actions,
(c) "nuts and bolts" investigative strategies, and
(d) maximizing the "bully pulpit" to prevent future victimization.

Instructor: Brian Moran

Presenting Audio/Video Evidence in Court
Room: 201 | **Type**: Lecture

While you may have no problem opening, playing, seeing, or hearing your audio/video evidence in your office, achieving the same results in a courtroom setting is sometimes a difficult task. Many courtrooms have outdated technology which can significantly hinder your ability to demonstrate key aspects of the recording. This session will cover common playback, display, and display problems. This session is perfect for investigators, examiners, and attorneys who want to know more about best practices when it comes to utilizing this type of evidence in court.

Instructors: Brewster Rolland-Keith

Submitting Mobile Device Evidence into Court – Encryption Issues
Room: 202 | **Type**: Cert

This presentation will discuss the importance of securing corroborating evidence from mobile device service providers. The legal requirements for obtaining such evidence will be discussed. The role of call detail records and the information provided in them will be explained. Conducting a direct examination of a witness testifying to the significance of such evidence will also be demonstrated.

Instructor: Justin Fitzsimmons

Session 8 | 3:45 PM: 5:00 PM
Descriptions

Mobile Device Forensics
Room: 101 | **Type**: Lecture

Mobile devices are nearly ubiquitous in today's society -- they are found at nearly every arrest and crime scene, and contain information relevant to an individual's pattern of behavior and personal contacts. Indeed, smartphones are so much more than phones -- they are portable Internet terminals.

This session will focus on the digital forensics process related to cell phones and mobile devices, particularly with initial device seizure in the field prior to transport to the lab

Instructor: Dr. Gary Kessler

Overcoming Persistent Smartphone Forensics Challenges
Room: 102 | **Type**: Lecture

A smartphone is never just a phone. Each iOS, Android, BlackBerry and Windows version might be found on any of several thousand types of smartphones and tablets, and dozens of mobile file systems exist across all device families. Passcodes and encryption continue to protect data and keep investigators away from crucial evidence. Extraction decryption, decoding and analysis are still the main challenges while data accuracy, forensic soundness and legal defensibility are as important as ever.

In this session, get an in-depth look at the technical challenges posed by device types, architectures, versions and device vendors' efforts to keep customer data private. Find out how about the existing capabilities and limitations while exploring the next tier and beyond.

Instructor: Ronen Engler

Middle East Terrorism and the Challenge's for Modern Societies
Room: 103 | **Type**: Lecture

This is a continuation from Session 7.

Instructor: Majid Hassan

Sex Trafficking & the Commercial Sexual Exploitation of Children
Room: 104 | **Type**: Cert

Attendees will learn the basics about human sex trafficking and the commercial sexual exploitation of children. Content includes misconceptions of human trafficking, venues for commercial sex work, domestic versus international trafficking, demand for sex, victimization involving commercial sex work, vulnerable populations and how vulnerabilities are exploited, organization of a trafficking enterprise, who the traffickers are, how traffickers/pimps control their victims and methods to identify

This is a continuation from Session 7.

Instructor: Sergeant Daniel Steele

Session 8 | 3:45 PM: 5:00 PM
Descriptions

Google
Room: 105/6 | **Type**: Lecture

This presentation provides an overview of Google's services and technologies, including Gmail, YouTube and Voice. In addition to describing the types of data available to law enforcement from those services and technologies, the presenters will review the policies and processes by which Google may provide data to law enforcement, consistent with state and federal law, including the Stored Communications Act.

Instructor: Cathy McGoff

RECON
Room: 107 | **Type**: Lecture

RECON for Mac OS X is simply one of the fastest way to conduct Mac Forensics. It automates what an experienced examiner would need weeks to accomplish in minutes. Join Manny Kressel, SUMURI's Managing Director of Services, for a DEMO of this product designed for both the novice and advanced forensic examiner and/or investigator.

Instructors: Manny Kressel

Autopsy 4: The Most Powerful Digital Forensics Platform You'll Find for Free
Room: 108 | **Type**: Lab

This lab is a continuation from Session 7.

Instructor: Dr. Brian Carrier

Previewing with WinFE in a lab environment
Room: 112 | **Type**: Lab

In recent years Windows Forensic Environment (WinFE) has become the standard for many law enforcement personnel who have a need to preview computers in a forensically sound manner. During this block we will explore the use of WinFE as a preview tool in a lab environment; however, we will also discuss its use for on-site preview. In addition to previewing, we will look at using WinFE to access some newer laptops and tablets, many of which now come configured 'UEFI Only' with no legacy support.

Instructor: John Riley

Volatile Data Collection - Local Machine and Network
Room: 113 | **Type**: Lab

In this hands-on lab, students will learn to use ProDiscover-IR to collect important system information and volatile artifacts from a live machine both locally and remotely over a network. Instructed by experienced investigators.This block was adapted from NW3C's Cybersecurity 235 - Basic Network Intrusion Investigations course http://www.nw3c.org/training/Computer-Crime/126

Instructors: Cynthia Gonnella | Michael Stern

Session 8 | 3:45 PM: 5:00 PM
Descriptions

Searching Facebook and Instagram
Room: 115 | **Type**: Lab

This lab is a continuation from Session 7.

Instructors: Lauren Wagner | Dean Chatfield

MDEC Digital Evidence Handler Certification Training
Room: 116 | **Type**: Lecture

This is a continuation from Sessions 4, 5, and 6 and continues in Session 8.

Instructor: Kevin Connolly

Microsoft and TASER Leverage the Cloud to Drive Safer Communities
Room: 117 | **Type**: Lecture

Body-worn and in-car video systems are some of the most important tools for law enforcement and the communities they serve - they help to solve crimes, increase transparency, and build trust in the community. For example, Axon cameras resulted in an 87.5% drop in complaints against officers for the city of Rialto, California, and the City of Pittsburgh Bureau of Police saw their numbers decrease by 74%. In this session you'll learn how Microsoft and TASER are leveraging the cloud to deliver breakthrough solutions for video capture, evidence management, analysis, and collaboration within agencies - all part of driving safer communities.

Instructors: Jeff King | Isaiah Fields

Collection of Digital Evidence: ECPA/ SCA
Room: 202 | **Type**: Lecture

If you learn that your suspect has used a social network provider, electronic mail service, cloud backup, or cellular service to commit a crime, do you know how to respond? Have you heard of the Federal Electronic Communications Privacy Act? What about the Stored Communications Act? Are you aware of search warrant statutes that deal specifically with the collection of digital evidence from these types of providers? If not, you should be, because the odds are that you will have to collect this type of evidence in the near future. The legal requirements can be confusing. Attendees to this session will learn how to demand records from electronic communication service providers in the legally appropriate manner.

Instructor: Justin Fitzsimmons

Day 3 Morning Agenda

Lecture | Lab | Cert | Prosecutor 3 Day

Day 2 Afternoon Sessions 7 and 8

Day 3 Morning Sessions 9, 10 and 11

Day 3 Afternoon Sessions 12 and 13

Bios

Sponsors/Exhibitors

Room	SESSION 9 8:30 AM - 9:40 AM	SESSION 10 9:50 AM - 11:00 AM	SESSION 11 11:10 AM - 12:20 PM
101	Tips & Tricks		Drone Forensics
102	Smartphone Malware: Identification & Examination	Advanced Browser Forensics - What your tools don't reveal	Smartphone Forensics: Third Party Application
103	Digital Forensics and Vehicle Systems	Beating the Backlog with New Forensic Technology	Boston Marathon Case Study
104	Inception of Radical Islamic Groups in the New York Area	ISIS - Tactics, Techniques and Procedures of Terrorist Attacks	The Overall Threat Picture
105/6	Expert Witness	Search Warrants 1	Search Warrants 2
107/8	Introduction to Social Media & Open Source Intelligence (OSINT) for Investigators		
112	Online Undercover Course		
113	Windows Virtual Machines for Use in Computer and Network Forensics	Processing Windows Event Logs for Timelining Criminal Cases	Gleaning Artifacts from Network Packet Capture (PCAP) Files
115	Introduction to WinFE		
116	MDEC Testimony Boot Camp		
117	Microsoft and TASER Leverage the Cloud to Drive Safer Communities	Microsoft Online, Safety & Services Overview	Technical Support Scams: Investigating and Preventing Tech Scams
201	Dealing with Proprietary CCTV DVR Video Files	Vehicle Make/Model Determination	
202	Authenticating Digital Evidence	Hot Topics Panel	Witness Prep

Lightning Talk Hosted by Rob Lee

TIFFANY BALLROOM - 12:30 PM - 1:45 PM

Session 9 | 8:30 AM: 9:40 AM
Descriptions

Tips & Tricks
Room: 101 | **Type**: Lecture

The Menz Brothers & Kip Loving class has been commonly known as the "tips and tricks" class for Internet investigations and digital forensics. The class will present and demonstrate current software and techniques for both investigation and forensic examinations that are not commonly known or are newly discovered or written. They will also present items that will become problems in the future for investigations. Those who attend the class also leave with a DVD of most of the software, web site.

This session continues in Session 10.

Instructors: Michael Menz | Detective Kipp Loving

Smartphone Malware: Identification and Examination (SANS FOR585)
Room: 102 | **Type**: Lecture

With the proliferation of mobile devices, mobile malware has become an increasing risk. Smartphones are increasingly becoming the target for malware as use of traditional desktop and notebook computers declines. While Android remains the most affected platform, all smartphones are at risk for malware. It's up to you to learn how to detect malware and determine how it's affecting the device. This lecture will cover detecting, decompiling, and determining what the malware is accessing. Different types of malware, the locations where they are commonly stored, as well as isolating malware will be covered. Not only will we discuss how malware can harm the user, but how the malware can be fruitful for your forensic investigation. We bet you didn't see that coming!

Instructors: Detective Cindy Murphy

Digital Forensics and Vehicle Systems
Room: 103 | **Type**: Lecture

This presentation will address the data stored in several different infotainment and telematics systems and touch on methods to acquire and analyze it. For example, vehicle Infotainment and Telematics systems store a vast amount of data such as recent destinations, favorite locations, call logs, contact lists, SMS messages, emails, pictures, videos, social media feeds, and the navigation history of everywhere the vehicle has been. These systems may also record door openings, gear shifts, etc.

Instructor: Ben LeMere

Session 9 | 8:30 AM: 9:40 AM
Descriptions

Inception of Radical Islamic Groups in the New York Area
Room: 104 | **Type**: Lecture

To present to the audience the circumstances that led to the opening of the first cases on the JTTF New York regarding the recruitment of "foreign fighters" against the Soviet Union in Afghanistan. How these cases addressed the first acts of terrorism in America attributed to the phenomenon of "radicalized Islam" and the threat of radicalization and returning foreign fighters. This lecture also explores the roots of Al Qaeda, Osama Bin Laden and the influence of Sheikh Omar Abdel Rahman (The Blind Sheikh) on the individuals who would later be responsible for the attack on the World Trade Center on February 26, 1993. This presentation also candidly discusses the mistakes that were made and lessons learned that were successfully applied in future cases. Also addressed is the fragile relationship between assets/sources, their handlers and management and how those relationships contribute to the success or failure of an operation.

Instructor: John Anticev

Expert Witness
Room: 105/106 | **Type**: Lecture

There is an art to testifying in court. For expert witnesses, court presentation skills are critical. In this section, Assistant District Attorney John Verner, Supervisor of Special Homicide Investigations at the Suffolk County District Attorney's Office , will discuss strategies, preparation, and the finer points of witness testimony from the lawyer's perspective.

Instructor: ADA John Verner

Introduction to Social Media & Open Source Intelligence (OSINT) for Investigators
Room: 107 | **Type**: Lab

The goal of the Introduction to Social Media & Open Source Intelligence (OSINT) for Investigators course is to provide those attending with the practical skills and knowledge necessary to use online open sources and social media websites during investigations.

While this is an introductory level course, basic computer and internet searching skills are a prerequisite.

Online open sources and popular social media websites including Facebook, Twitter, and Instagram often contain valuable information and evidence related to an investigation. This information can assist an investigator with identifying potential suspects, accomplices, witnesses, victims, communications, and establishing timelines.

A combination of classroom instruction and live, online practical exercises will provide attendees with the techniques used to search open sources and social media successfully. Each attendee will be provided with a laptop and internet access to perform instructor-led practical exercises.

This lab continues in Sessions 10, 11, 12, and 13.

Instructors: Trooper Brian Gavioli | Ed Bradstreet

Session 9 | 8:30 AM: 9:40 AM
Descriptions

On-Line Undercover Course
Room: 112 | **Type**: Lab

This accredited course is for government officers who operate undercover on-line across a range of law enforcement units. It is widely taught across United Kingdom government bodies with investigative roles. The course will teach a suite of infiltration and penetration techniques which can typically be used against individuals or groups to combat serious and organised crime, terrorism and pedophile groups.

This lab continues in Sessions 10, 11, 12, and 13.

Instructor: Bren Jose

Windows Virtual Machines for Use in Computer and Network Forensics
Room: 113 | **Type**: Lab

In this hands-on lab, students will simulate the creation of a Windows virtual machine using Windows built-in Hypervisor technology, and work with a pre-built Hypervisor VM. This is an important skill for forensic examiners, as it allows them to work a case while maintaining control of contraband at all times and protects their underlying forensic machine from malware. Instructed by experienced investigators. Adapted from NW3C's Cybersecurity 235 - Basic Network Intrusion Investigations course.

Instructors: Cynthia Gonnella | Michael Stern

Introduction to Windows Forensic Environment (WinFE) (Part 1)
Room: 115 | **Type**: Lab

The Windows Forensic Environment (WinFE) is a bootable forensic environment. WinFE does not mount the suspect's hard drive which will allow investigators to operate in a traditional Windows environment and run their preview tools against a suspect computer. This lab and lecture will provide the attendee with the skills and software necessary to create a WinFE image which can be booted by either CD or USB device. Students will also have the opportunity to practice booting a "suspect computer" with their WinFE and run preview tools. **Note: Due to Windows licensing rules students will create their cd and USB thumb drives using a 30-day evaluation copy of Windows.

Instructors: Dean Chatfield | Lauren Wagner

Testimony Boot Camp
Room: 116 | **Type**: Lecture

The Massachusetts Digital Evidence Consortium ("MDEC") will feature three modules of the Digital Evidence Certification Program. MDEC is a group of subject matter experts who meet regularly to resolve issues relating to standards, protocols, training and education, tool testing, authentication, and a variety of other issues related to computer forensics. Selected digital evidence analysts will take part in a mock direct and cross examination conducted by cyber crime prosecutors from across the country. A discussion and critique with the participants will follow. This exam continues through Sessions 5, 6, 7, and 8. Attendees may participate as "members of the jury or public."

Instructor: Attorney Christine Tetreault

Session 9 | 8:30 AM: 9:40 AM
Descriptions

Microsoft and TASER Leverage the Cloud to Drive Safer Communities
Room: 117 | **Type**: Lecture

Body-worn and in-car video systems are some of the most important tools for law enforcement and the communities they serve - they help to solve crimes, increase transparency, and build trust in the community. For example, Axon cameras resulted in an 87.5% drop in complaints against officers for the city of Rialto, California, and the City of Pittsburgh Bureau of Police saw their numbers decrease by 74%. In this session you'll learn how Microsoft and TASER are leveraging the cloud to deliver breakthrough solutions for video capture, evidence management, analysis, and collaboration within agencies - all part of driving safer communities.

Instructors: Jeff King | Isaiah Fields

Dealing with Proprietary CCTV DVR Video Files
Room: 201 | **Type**: Lecture

Downloading video evidence from a DVR can sometimes be a difficult process, but getting those exported files to play on your computer can be just as challenging. In this session, we will discuss how to interrogate these types of files in order to find the correct method of playback and/or conversion.

Instructors: Brewster Rolland-Keith

Authenticating Digital Evidence
Room: 202 | **Type**: Cert

This presentation covers the various types of evidence that investigators can gather from cyberspace and cellular phone providers. The audience is shown case law examples for authenticating emails, chats, and other technological evidence. The presentation also gives examples of what type of witnesses are needed to lay the proper foundation for the admission of digital evidence.

Instructor: Howard Wise

Session 10 | 9:50 AM: 11:00 AM
Descriptions

Tips & Tricks
Room: 101 | **Type**: Lecture

The Menz Brothers & Kip Loving class has been commonly known as the "tips and tricks" class for Internet investigations and digital forensics. The class will present and demonstrate current software and techniques for both investigation and forensic examinations that are not commonly known or are newly discovered or written. They will also present items that will become problems in the future for investigations. Those who attend the class also leave with a DVD of most of the software, web site.

This session is a continuation from Session 9.

Instructors: Michael Menz | Detective Kipp Loving

Advanced Browser Forensics - What your tools don't reveal (SANS FOR408)
Room: 102 | **Type**: Lecture

With the increasing use of the Web and the shift toward Web-based applications and cloud computing, browser forensic analysis is a critical skill. However, most forensic tools barely scratch the surface when it comes to properly extracting browser-related data during an exam. During this section from our popular course, FOR408, the investigator will comprehensively explore Web browser evidence created during the use of Internet Explorer, Firefox, and Google Chrome. The skills taught here, such as SQLite and ESE database parsing, allow investigators to extend these methods to nearly any browser they encounter. The analyst will learn how to examine every major artifact stored by the browser, including cookies, and how to visit and download history, Internet cache files, browser extensions, and form data. We will show you how to find these files and identify the common mistakes investigators make when interpreting browser artifacts. You will also learn how to analyze some of the more obscure browser artifacts such as session restore, tracking cookies, and private browsing remnants.

Instructors: Rob Lee

Beating the Backlog with New Forensic Technology
Room: 103 | **Type**: Lecture

The current landscape of law enforcement investigations includes an ever-increasing number of cases containing digital evidence. This, coupled with increasing data storage device sizes and stagnant budgets for hiring additional personnel, leaves law enforcement organizations struggling to dig themselves out of large digital evidence case backlogs. Learn how the latest Nuix technologies and workflows can be leveraged to recover from the digital evidence case backlog and conduct more efficient and quicker digital investigations moving forward.

Instructor: Tim Moniot

ISIS - Tactics, Techniques and Procedures of Terrorist Attacks
Room: 104 | **Type**: Cert

This presentation will explore the TTPs (tactics, Techniques and procedures) of ISIS/AQ. Starting with a review of the recent attacks in Brussels and Paris to the capabilities of ISIS/AQ. A discussion on external operations, targeting, tradecraft, motivation, recruitment, criminal enterprises, and source recruitment.

Instructor: Vaughn Forest

Session 10 | 9:50 AM: 11:00 AM
Descriptions

Search Warrants 1
Room: 105/6 | **Type**: Lecture

Applying for search warrants that involve searching for and seizing digital evidence at physical locations requires both knowledge of traditional search warrant law and awareness of the latest cyber law issues. This session will include a review of traditional search warrant legal principles as well as an extended discussion about how these principles apply to digital evidence. Attendees will also receive the latest search warrant language used by cyber crime investigators in Massachusetts.

Instructor: AAG Allyson Portney

Introduction to Social Media & Open Source Intelligence (OSINT) for Investigators
Room: 107 | **Type**: Lab

This lab is a continuation from Session 9 and continues in Session 11, 12, and 13.

Instructor: Trooper Brian Gavioli | Ed Bradstreet

On-Line Undercover Course
Room: 112 | **Type**: Lab

This lab is a continuation from Session 9 and continues in Session 11, 12, and 13.

Instructor: Bren Jose

Processing Windows Event Logs for Timelining Criminal Cases
Room: 113 | **Type**: Lab

In this hands-on lab, students will use Fire-Eye Mandiant's Redline to collect and process data to tell a story of how files came to be on a particular machine. This skill is very important when working computer facilitated criminal cases. Students learn to timeline Internet history, file downloads, program installations, programs run, files accessed, and by what account. Instructed by experienced investigators. Adapted from NW3C's Cybersecurty 235 - Basic Network Intrusion Investgations course.

Instructors: Cynthia Gonnella | Michael Stern

Introduction to Windows Forensic Environment (WinFE) (Part 2)
Room: 115 | **Type**: Lab

This lab is a continuation from Session 9 and continues in Session 11.

Instructors: Dean Chatfield | Lauren Wagner

Testimony Boot Camp
Room: 116 | **Type**: Cert

This session is a continuation from Session 9 and continues in Sessions 12 and 13.

Instructor: Massachusetts Digital Evidence Consortium

Session 10 | 9:50 AM: 11:00 AM
Descriptions

Microsoft Online, Safety & Services Overview
Room: 117 | **Type**: Lecture

This presentation will provide an overview of the major online services which Microsoft provides to customers including Outlook.com (Hotmail), OneDrive, Skype and XBox. For each service, you will learn what data may be available with the appropriate service of legal process, where and how to serve legal process, user notification policies, requirements for threat-to-life emergency requests, and response expectations.

Instructors: Tracy Ingle

Vehicle Make/Model Determination
Room: 201 | **Type**: Lecture

Attempting to determine the make/model of a particular vehicle depicted in images and video is a frequent task for detectives, investigators and forensic personnel. Despite the fact the images/video used in these types of exams are often of low quality, with the right workflow and techniques it is possible to significantly reduce the number of possible types of vehicles. In some cases, a vehicle may even be narrowed down to a specific make/model or trim level.

Instructor: Brewster Rolland-Keith

Hot Topics in Cyber Crime Law
Room: 202 | **Type**: Cert

The evolving issues of case law and digital evidence will be discussed during this session. The impact of the passage and implementation of CAL ECPA will be discussed.

Instructors: Howard Wise | Abigal Abraham | Margaret Ogarek

Session 11 | 11:10 AM: 12:20 PM
Descriptions

Introduction to Drone Forensics
Room: 101 | **Type**: Lecture

This course will introduce you to the term "Drones" and that it covers from small copters to full size planes, automobiles, boats and robots. You'll learn where evidence and artifacts can be found and where resources are to assist in forensics examinations.

Instructors: Michael Menz | Detective Kipp Loving

Smartphone Forensics - Third Party Application (SANS FOR585)
Room: 102 | **Type**: Lecture

As use of third-party apps become increasingly popular, the impact they have on investigations is substantial. When conducting a digital forensic investigation involving a smartphone, a common misconception is that if a tool doesn't parse third party application data, there is no data to be found, or that data from 3rd party apps advertised as encrypted can't be interpreted. The reality, however, is often that the tool is not looking in the correct location or cannot properly decode the data. How 3rd party application data is stored varies greatly depending on the device itself and the installed operating system. To stay current and ensure cases are not compromised as a result of missed evidence, investigators must take the time to learn how and where to find third party-app data. In doing so investigators skills will be in greater demand as they will be able to find and successfully interpret critical evidence that others are overlooking. In this session, we will explore tools and techniques that allow the examiner to dive into 3rd party application data when it's not fully parsed by their forensic tool.

Instructors: Detective Cindy Murphy

Boston Marathon Case Study
Room: 103 | **Type**: Lecture

The briefing will include an overview of the investigative highlights of the Boston Marathon Bombing investigation and will include discussions of digital media evidence collection, trial preparation and testimony. Will also provide insight to the NCCC audience regarding the digital media handling challenges and investigative strategy surrounding the events of April 15, 2013 and the Boston Marathon Bombing Investigation while highlighting the lessons learned and after action response.

Instructors: SSA Kevin Swindon | John Petrozzelli

The Overall Threat Picture
Room: 104 | **Type**: Cert

The presentation will introduce the S015 cyber operations unit and then will cover an over view of the methods Islamic fighter have used to broadcast and communicate and some emerging threats that have been detected over in the UK. It will show some case studies which our unit have helped to bring to court, whilst highlighting some of the issues we have encountered, namely dealing with returnees from Syria , and an example of a plot our organization helped to disrupt.

Instructors: A. Robertson

Session 11 | 11:10 AM: 12:20 PM
Descriptions

Search Warrants 2
Room: 105/106 | **Type**: Lecture

Evidence held by third-party email, internet service, cellular, and social network providers is becoming increasingly critical to criminal investigations. Police and prosecutors are required to use legal process to obtain subscriber information and account content from these providers. Attendees will obtain an overview of the Stored Communications Act and the various processes for demanding records from providers. Attendees will also hear about the latest approaches to search warrants to obtain social network, email, and cell phone account content.

Instructor: Allyson Portney

Introduction to Social Media & Open Source Intelligence (OSINT) for Investigators
Room: 107/8 | **Type**: Lab

This lab is a continuation from Session 9 and 10 and continues in Sessions 12 and 13.

Instructor: Trooper Brian Gavioli | Ed Bradstreet

On-Line Undercover Course
Room: 112 | **Type**: Lab

This session is a continuation from Sessions 9 and 10 and continues in Sessions 12 and 13.

Instructor: Bren Jose

Gleaning Artifacts from Network Packet Capture (PCAP) files
Room: 113 | **Type**: Lab

In this hands-on lab, students will use Wireshark and Network Miner to collect artifacts of importance from packet capture files (network traffic). This is an important skill when investigating any computer network related cases. Students will data mine network traffic for graphic files, screen names, and keywords. Instructed by experienced investigators. Adapted from NW3C's Cybersecurity 235 - Basic Network Intrusion Investigations http://www.nw3c.org/training/Computer-Crime/126

Instructors: Cynthia Gonnella | Michael Stern

Introduction to Windows Forensic Environment (WinFE) (Part 3)
Room: 115 | **Type**: Lab

This lab is a continuation from Sessions 9 and 10. Pre-registration is required for admittance into this lab.

Instructors: Dean Chatfield | Lauren Wagner

Testimony Boot Camp
Room: 116 | **Type**: Cert

This session is a continuation from Sessions 9 and 10 and continues in Sessions 12 and 13.

Instructor: Massachusetts Digital Evidence Consortium

Session 11 | 11:10 AM: 12:20 PM
Descriptions

Technical Support Scams- Investigating and Preventing Tech Scams

Room: 117 | **Type**: Lecture

This panel discussion will cover the scope of the tech support scam problem faced by law enforcement today, currently estimated as affecting 3.3 million consumers each year with an average financial loss of $454 per consumer, or $1.5 billion. Part two will be devoted to identifying practical investigative approaches and available resources to hold tech scammers accountable for their illegal acts, including:

(a) resources for identification of victims,
(b) forming multi-jurisdictional investigative teams v. individual actions,
(c) "nuts and bolts" investigative strategies, and
(d) maximizing the "bully pulpit" to prevent future victimization.

Instructor: Brian Moran

Witness Prep

Room: 202 | **Type**: Cert

There is an art to testifying in court. For expert witnesses, court presentation skills are critical. In this section, Assistant District Attorney John Verner, Supervisor of Special Homicide Investigations at the Suffolk County District Attorney's Office , will discuss strategies, preparation, and the finer points of witness testimony from the lawyer's perspective

Instructor: John Verner

Day 3 Afternoon Agenda

Lecture | Lab | Cert | Prosecutor 3 Day

Day 2 Afternoon Sessions 7 and 8

Day 3 Morning Sessions 9, 10 and 11

Day 3 Afternoon Sessions 12 and 13

Bios

Sponsors/Exhibitors

Room	SESSION 12 2:15 PM - 3:30 PM	SESSION 13 3:45 PM - 5:00 PM
101	Live Forensics and Locked Computers	How Tableau and EnCase Forensic Can Help You Complete Digital Investigations
102	What you need to know about Windows 10 Forensics	Child Victim Age Estimation from Images and Videos
103	School Threats	Building and Optimizing a Forensic Workstation
104	How to find ISIL Supporters Online	What does ISIL/AQ ideology Look Like?
105/6	Social Media and Intelligence Gathering	Internet of Things
107	Introduction to Social Media & Open Source Intelligence (OSINT) for Investigators	
112	Online Undercover Course	
113	Volatile Data Collection (Local Machine & Network)	Windows Virtual Machines for Use in Computer and Network Forensics
115	OsTriage	
116	MDEC Testimony Boot Camp	
117	Community on Patrol: Citizens as Sensors to Fight Terrorism, Reduce Crime, & Improve Public Safety	How Machine Learning is Facilitating Video Management and Public Records Requests
201	Recovery of Video Evidence Using DVR Examiner (Hands On)	
202	Trial Demo – Live Direct and Cross of Digital Forensic Expert (Mobile Device Case)	

CONFERENCE ADJOURNS - 5:00 PM

Session 12 | 2:15 PM: 3:30 PM
Descriptions

Live Forensics in Locked Computers
Room: 101 | **Type**: Lecture

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 answer these questions.

Instructors: Kristopher Carver | Jeffry Gummeson

What you need to know about Windows 10 Forensics (SANS FOR408)
Room: 102 | **Type**: Lecture

Windows 10 has dominated the new PC market for the past year. This session will focus on artifacts that have changed and updated from the previous versions of Windows. It is highly likely investigators will encounter a Windows 10 system more quickly than any other Microsoft Operating System that has been released in the past 10 years. Are your tools compatible? Are your techniques still valid? What are the most important take-aways that each investigator must know before engaging in Windows 10 analysis? Come find out in this session.

Instructors: Rob Lee

School Threats
Room: 103 | **Type**: Lecture

School threats will cover your response to bomb threats and how to start your investigation. Covered in the lecture will be common trends using robo calling and the dark web. We will also discuss trace and traps on phone numbers, tracking the number to a location through free online tools and judicial process. Also covered will be tracking internet based threats. With mass threats being the tread in today's world, evaluation and reporting will also be addressed.

Instructor: Kevin Connolly

How to find ISIL Supporters Online
Room: 104 | **Type**: Cert

This presentation will be a discussion on using social media to locate those that have taken up ISIL's call to arms. From the importance of setting up a process, to the nuts and bolts of using social media tools to identify ISIL's supporters in your area and finally to assessing subjects.

Instructor: Kevin Branzetti

Session 12 | 2:15 PM: 3:30 PM
Descriptions

Social Media and Intelligence Gathering
Room: 105/106 | **Type**: Lecture

This course will consider the vast data and intelligence opportunities available through social media. Exploring a range of tools and their respective capacity will provide attendees with an objective assessment of how intelligence about suspects can be secured. Examples through cases will be used to illustrate the value of using search tools and a simple fictitious operation will be used to identify how an intelligence gathering plan is so essential for success.

Instructor: Stuart Hyde

Introduction to Social Media & Open Source Intelligence (OSINT) for Investigators
Room: 107/8 | **Type**: Lab

This lab is a continuation from Session 9, 10 and 11 and continues in Session 13.

Instructor: Trooper Brian Gavioli | Ed Bradstreet

On-Line Undercover Course
Room: 112 | **Type**: Lab

This lab is a continuation from Sessions 9, 10, 11 and continues in Session 13.

Instructor: Bren Jose

Volatile Data Collection - Local Machine and Network
Room: 113 | **Type**: Lab

In this hands-on lab, students will learn to use ProDiscover-IR to collect important system information and volatile artifacts from a live machine both locally and remotely over a network. Instructed by experienced investigators.This block was adapted from NW3C's Cybersecurity 235 - Basic Network Intrusion Investigations course http://www.nw3c.org/training/Computer-Crime/126

Instructors: Cynthia Gonnella | Michael Stern

osTriage
Room: 115 | **Type**: Lab

This hands-on lab will provide instruction on osTriage, where to get it, how to use it, and how it can enhance on-scene previews to give you the most information in the shortest amount of time. osTriage will quickly find, extract, and display key information from a computer which will enable you to get a better first interview of your subject and conduct a better search of the subject premises.

Instructor: Jeffrey Rich

Testimony Boot Camp
Room: 116 | **Type**: Cert

This session is a continuation from Sessions 9, 10, 11 and continues in Session 13.

Instructor: Massachusetts Digital Evidence Consortium

Session 12 | 2:15 PM: 3:30 PM
Descriptions

Community on Patrol: Citizens as Sensors to Fight Terrorism, Reduce Crime, and Improve Public Safety

Room: 117 | **Type**: Lecture

With recent terrorist attacks, law enforcement agencies are investing in new sensor based technologies (surveillance systems, drones, etc.) and location-based data feeds to gather intelligence and respond proactively to public safety concerns. One challenge faced however, is how to tap into the vast amount of data being generated by private citizens. Videos, photos, and social media posts, created using smartphones, have the potential to provide first responders with information that could aid in their efforts. In this session, hear how the Miami-Dade police department has developed a new smartphone application Community On patrol, designed to deputize the counties 2.6 million residents and improve community relations.

Instructors: Jeff King

Recovery of Video Evidence Using DVR Examiner (Hands On)

Room: 201 | **Type**: Lab

Recovering video evidence from CCTV digital video recorders (DVRs) can be a difficult process, but it doesn't have to be. DVR Examiner is a software solution for acquiring video and metadata from CCTV DVRs in a forensically sound manner. We will demonstrate the forensic workflow and also briefly discuss the technical processes behind DVR Examiner. The remainder of the session will be dedicated to hands-on use of DVR Examiner in the form of guided walkthroughs and practical exercises.

Instructors: Jimmy Schroering | Brewster Rolland-Keith

Trial Demo: Live Direct and Cross of Digital Forensic Expert

Room: 202 | **Type**: Lab

Do you need to put an expert digital evidence analyst on the stand in your case? Do you need to cross-examine one. Experienced cyber prosecutors conduct a mock direct and cross-examination of an expert analyst.

Instructors: Howard Wise | Margaret Ogarek | Steve Devlin

Session 13 | 3:45 PM: 5:00 PM
Descriptions

How EnCase Forensic and Tableau Can Help You Complete Investigations

Room: 101 | **Type**: Lecture

See how EnCase Forensic and Tableau forensic hardware can help you complete investigations, from triage to reporting. Using a sample case we will highlight some of our newest capabilities, including major improvements to Hash analysis, filtering, and our Project VIC integrated workflow. We'll also talk about how Tableau hardware, including the Tableau Password Recovery product, can expedite investigations. Lastly, we will provide a preview of what is coming from Guidance for the rest of 2016.

Instructor: Steve Salinas

A Multidisciplinary Approach to the Estimation of Victim Age in Child Pornography and Child Sexual Exploitation Investigations

Room: 102 | **Type**: Lecture

The Internet and digital photography technologies have indisputably played a significant role in proliferation and availability of child pornography and thus in the number of child pornography and child exploitation investigations. As a consequence, digital forensic examiners are increasingly tasked with investigating and assisting in the prosecution of criminal child pornography and sexual exploitation cases. The examiner therefore is often placed in the position of acting as a gate keeper to the criminal justice system when making the determination as to whether or not an image or movie features an individual whose age fits their jurisdiction's statutory definition of 'child' or 'minor' and consequently whether the subject media is illegal or not. How good are we at age estimation? At what stage does it become difficult to tell the difference between a child and an adult? What are the perceptual cues that we can use and articulate to make the best age estimates possible? Det. Murphy will present the content of her dissertation research and findings regarding our ability to estimate victim age based upon digital images and will provide a practical framework and method for child victim age estimation.

Instructors: Detective Cindy Murphy

Building and Optimizing a Forensic Workstation

Room: 103 | **Type**: Lecture

Modern forensic examiners face tremendous technological hurdles; when having to process large storage devices, attempting to defeat encryption, recovering passwords and indexing enormous amounts of data. Selecting and using the proper equipment is essential when faced with these daily tasks. Knowing what components to select and how to properly configure a forensic workstation for the most popular forensic software suites can mean the difference between waiting for several days or just a few hours. Join Manny Kressel, SUMURI's lead architect of their popular TALINO Forensic Workstations, as he provides tips and tricks for constructing and properly configuring a forensic workstation for maximum efficiency and speed.

Instructor: Manny Kressel

Session 13 | 3:45 PM: 5:00 PM
Descriptions

What does ISIL/AQ ideology Look Like?
Room: 104 | **Type**: Cert

In this session we will compare and contrast AQ and ISIS, learn how they communicate between fighters and people they inspire, how to engage them online and in real world, how to recognize their official media outlets, and the main reasons why people join ISIS and AQ.

Instructor: Sergeant Driton Gashi

Internet of Things
Room: 105/6 | **Type**: Lecture

This course explores the dilemma created through our willingness to connect everyday, and sometimes very surprising devices, to the Internet and the unintended consequences that could result. Working on the basis that anything connected to the Internet can be hacked this course will raise questions about new vulnerabilities and opportunities for criminal activity. A preventative strategy will be discussed alongside raising officer and citizen awareness of future potential risk threat and harm.

Instructor: Stuart Hyde

Introduction to Social Media & Open Source Intelligence (OSINT) for Investigators
Room: 107 | **Type**: Lab

This lab is a continuation from Session 9, 10, 11 and 12. Pre-registration is required for admittance into this lab.

Instructor: Trooper Brian Gavioli | Ed Bradstreet

On-Line Undercover Course
Room: 112 | **Type**: Lab

This lab is a continuation from Sessions 9, 10, 11 and 12.

Instructor: Bren Jose

Windows Virtual Machines for Use in Computer and Network Forensics
Room: 113 | **Type**: Lab

In this hands-on lab, students will simulate the creation of a Windows virtual machine using Windows built-in Hypervisor technology, and work with a pre-built Hypervisor VM. This is an important skill for forensic examiners, as it allows them to work a case while maintaining control of contraband at all times and protects their underlying forensic machine from malware. Instructed by experienced investigators. Adapted from NW3C's Cybersecurity 235 - Basic Network Intrusion Investigations course.

Instructors: Cynthia Gonnella | Michael Stern

osTriage
Room: 115 | **Type**: Lab

This lab is a continuation from Session 12.

Instructor: Jeffrey Rich

Session 13 | 3:45 PM: 5:00 PM
Descriptions

Testimony Boot Camp
Room: 116 | **Type**: Cert

This session is a continuation from Sessions 9, 10, 11 and 12.

Instructor: Massachusetts Digital Evidence Consortium

How Machine Learning is Facilitating Video Management and Public Records Requests
Room: 117 | Lecture

Video in law enforcement has become a powerful tool in how agencies protect themselves, as well as private citizens. Challenges exist however, in how agencies effectively manage all of this of this video - Curating thousands of hours of video can be a costly and resource intensive process. Agencies are looking to new technologies to help them automate their video management processes: Extracting spoken content, image stabilization, object recognition, redacting (blurring), sentiment and motion detection. In this session, learn how agencies are addressing these and other challenges by leveraging new Cloud based machine learning technologies, that offer advanced video analytics and management capabilities.

Instructor: Jeff King | John Newsom

Recovery of Video Evidence Using DVR Examiner (Hands On)
Room: 201 | **Type**: Lab

This session is a continuation from Session 12.

Instructors: Jimmy Schroering | Brewster Rolland-Keith

Trial Demo: Live Direct and Cross of Digital Forensic Expert
Room: 202 | **Type**: Lab

This session is a continuation from Session 12.

Instructors: Howard Wise | Margaret Ogarek | Steve Devlin