

-
-
-
-
-
-
-
-

ISS World Asia is the world's largest gathering of Asian Law Enforcement, Intelligence and Homeland Security Analysts as well as Telecom Operators responsible for Lawful Interception, Hi-Tech Electronic Investigations and Network Intelligence Gathering.

ISS World Programs present the methodologies and tools for Law Enforcement, Public Safety and Government Intelligence Communities in the fight against drug trafficking, cyber money laundering, human trafficking, terrorism and other criminal activities conducted over today's telecommunications network and the Internet.

[Track 1: Lawful Interception and Criminal Investigation Training](#)

[Track 2: Big Data Analytics and Social Network Monitoring Training](#)

[Track 3: Distilling Cyber Threat Information into Actionable Intelligence Training](#)

[Track 4: Encrypted Traffic Monitoring and IT Intrusion Product Training](#)

[Track 5: LEA, Defense and Intelligence Analyst Training and Product Demonstrations](#)

[Track 6: Social Network Monitoring and Big Data Analytics Training and Product Demonstrations](#)

[Track 7: Mobile Signal Intercept and Electronic Surveillance Training and Product Demonstrations](#)

[Pre-Conference Seminars and Tutorials \(Tuesday, 2 December 2014\)](#)

ISS World Asia - Conference Agenda at a Glance 2014

Tuesday, 2 December 2014

Pre-Conference Seminars and Tutorials

Seminar #1

8:30-16:30

Online Social Media and Internet Investigations

Presented by *Charles Cohen, **Cohen Training and Consulting, LLC***

*Charles Cohen also holds the position of Commander, Cyber Crimes Investigative Technologies Section, **Indiana State Police, USA***

8:30-9:30: Session 1 of 6

The role of Online Social Media OSINT in Predicting and Interdicting Spree Killings: Case Studies and Analysis

9:45-10:45: Session 2 of 6

OSINT and Criminal Investigations

11:00-12:00: Session 3 of 6

Metadata Exploitation in Criminal Investigations

13:00-14:00: Session 4 of 6

EXIF Tags and Geolocation of Devices for Investigations and Operational Security

14:15-15:15: Session 5 of 6

Case Studies in Metadata Vulnerability Exploitation and Facial Recognition

15:30-16:30: Session 6 of 6

What Investigators Need to Know about Emerging Technologies Used to Hide on the Internet

Seminar #2

8:30-16:30

Understanding ISS Technologies and Products Deployed in Telecommunications Networks and Monitoring Centers for Law Enforcement and Intelligence Analysts

Presented by: *Dr. Jerry Lucas, President, **TeleStrategies***

This one day pre-conference seminar covers the spectrum of ISS Technologies and Products deployed in today's fixed wire, mobile wireless and Internet Service Provider networks and LEA Monitoring and Intelligence Gathering Centers. This all day seminar is ideal for those law enforcement, public safety and intelligence analysts who need an understanding of the ISS technologies to be discussed in the conference sessions and the ISS products displayed at the exhibit hall as well as an understanding of the buzz words and jargon used by telecom operator engineers and their vendors.

08:30-10:45

Introduction to Telecom Infrastructure, Interception and Related ISS Products

11:00-14:00

Understanding Mobile Wireless Infrastructure, Interception and Related ISS Products

14:15-16:30

Understanding the Internet, Interception and Related ISS Products

Seminar#3

8:30-16:30

Practitioners Guide to Internet Investigations

Presented by: *Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement, UK Police*

The aim of this 1 day seminar is to take the attendees from the basics of understanding the internet, how to find data, through to a full understanding of best practice of an internet investigator, having awareness and knowledge of all the tools available to achieve this.

This is exclusively Law Enforcement only, as Practical examples, covert and investigative methods will be given throughout the seminar.

8:30-9:30

The World Wide Web and the Internet

9:45-10:45

Recognizing Traffic Data

11:00-12:00

WIFI and Mobile Data

13:00-14:00

Emerging Technologies, Masking Tech and Tools

14:15-15:15

Advanced Techniques in Tracing Suspects

15:30-16:30

Open Source Intelligence Training (OSINT)

Wednesday, 3 December 2014

Welcoming Remarks

8:15-8:30

Tatiana Lucas, ISS World Program Director, TeleStrategies

8:30-9:00

**Top Ten Internet Challenges Facing Law Enforcement and the Intelligence Community
ISS World Asia has Solutions**

Dr. Jerry Lucas, President, TeleStrategies

ISS World Americas Exhibit Hours:

Wednesday, 3 December 2014

Hours: 10:00 - 17:00

Thursday, 4 December 2014

Hours: 9:30 - 12:30

Track 1: Lawful Interception and Criminal Investigation Training

This track is for Telecom Operators and Law Enforcement/Intelligence/Defense Analysts who are responsible for specifying or developing lawful intercept network infrastructure.

Wednesday, 3 December 2014

- | | |
|-------------|--|
| 9:00-9:30 | Newest trends and technologies in Lawful Interception <i>Presented by trovicor</i> |
| 9:30-10:00 | Today's Interception in an Encrypted, Social and Clouded World <i>David Vincenzetti, CEO, Hacking Team</i> |
| 11:30-12:00 | Demystifying SSL/TOR Interception: Attack Case History and State-of-the-art <i>David Vincenzetti, CEO, Marco Valleri, CTO, Alberto Ornaghi, Software Architect</i> |
| 12:00-12:30 | LI Umbrella Solutions <i>Jörg Schomburg, Utimaco TS GmbH</i> |
| 13:30-14:00 | Lawful Interception in 4G Wireless Networks <i>Rene Nitzinger, Utimaco TS GmbH</i> |
| 14:00-14:30 | Mass Voice and IP Intercept in 3g and LTE networks <i>Presented by iSolv Technologies</i> |
| 16:15-17:15 | Enterprise-Level Intercept Technology for Edge Users <i>Presented by Ultra Electronics, ProLogic</i> |

Thursday, 4 December 2014

- | | |
|-------------|--|
| 8:30-9:30 | Industry Developments Changing the LI Landscape <i>Tony Rutkowski, Executive VP, Yaana Technologies</i> |
| 10:30-11:00 | DeepInsight story - How to gather and use Mass Intelligence? <i>Presented by Sinovatio</i> |
| 11:00-11:30 | Understanding the challenge of full VoLTE visibility on 10/40/100G lines in the <i>Presented by FiberBlaze</i> |
-

Track 2: Big Data Analytics and Social Network Monitoring Training

This track is for Intelligence Analysts and Law Enforcement agents who have to “connect the dots” between people, places and other entities by searching through massive amounts of unstructured data from various sources using visual analytics, semantic technologies, data mining, OSINT and other intelligence gathering tools and techniques

Tuesday, 2 December 2014

8:30-16:30

Online Social Media and Internet Investigations

Charles Cohen, Cohen Training and Consulting, LLC

Wednesday, 3 December 2014

15:00-15:30

Making Sense of the Deep Web: A Practical, Nationwide Solution Case Study

Niv Blond, Director of Sales and Marketing, 3i-MIND

15:30-16:00

Collecting Data from all parts of the Web for Intelligence

David Turner, Vice President of Asia Pacific, Kapow Software, a Kofax company

Jez Nelmes, Chief Architecture, BAE Systems Applied Intelligence

Track 3: Distilling Cyber Threat Information into Actionable Intelligence

This track addresses how to detect cyber threats in real-time and share threat information with private enterprises, government agencies as well as other telecom operators. This track is open to telecom operators, private enterprise person with security and investigation responsibilities, all government attendees and ISS vendors.

Tuesday, 2 December 2014

13:00-14:00

Zero-day attacks - Finding Advanced Threats in ALL of Your Data

C F Chui, Solutions Architect, APAC, Arbor Networks

14:15-15:15

Changing Landscape of Cyber Security Threats - Are you ready?

Presented by Palo Alto Networks

15:30-16:30

Thinking Like an Attacker (Not an Auditor)

Philippe Alcoy, Technical Director, International, Rapid7

Track 4: Encrypted Traffic Monitoring and IT Intrusion Product Training

This track is only open to Law Enforcement, Public Safety and Government Intelligence Community Attendees

Tuesday, 2 December 2014

13:00-14:00 **Encryption of mass-communication changed the game's rules: Remote Stealth S**
Presented by AGT

Wednesday, 3 December 2014

9:00-10:00 Session **ONE. Targeted Deployment of Surveillance Capabilities**
A *Presented by FinFisher*

9:00-10:00 Session **Tactical IP Intercept for HTTPS Monitoring & Remote Intrusion**
B *Jitendra Verma, Director, Business Development, ClearTrail Technologies*

11:30-12:00 Session **Encryption of mass-communication changed the game's rules, learn how to stay al**
A **Stealth Surveillance**
Presented by AGT

11:30-12:30 Session **Unconventional IP Monitoring**
B *Presented by IPS*

13:30-14:30 Session **Intruding Personal Devices with Remote Control System: Live Demo of Latest Att**
A **Gathering Techniques**
Marco Valleri, CTO, Alberto Ornaghi, Software Architect, Fabrizio Cornelli, QA Mana

13:30-14:30 Session **Encryption, Non-Decryption & Way Forward**
B *Naveen Jaiswal, Head - R&D, Vehere*

15:00-16:00 Session **FinFisher™: Maximum Impact - The Evolution of IT Investigation**
A *Presented by FinFisher*

15:00-16:00 Session **DARK EAGLE: Fully configurable remote IT Intrusion Solution; Case studies, De**
B **latest intrusion techniques**
Presented by GR Sistemi

Thursday, 4 December 2014

8:30-9:30 Session B **Methodologies and Instruments for Remote IT Intrusion**
Presented by RCS

Track 5: LEA, Defense and Intelligence Analyst Training and Product Demonstrations

This training is only open to Law Enforcement, Public Safety and Government Intelligence Community Attendees.

Tuesday, 2 December 2014

8:30-16:30

Practitioners Guide to Internet Investigations

Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement

Wednesday, 3 December 2014

9:30-10:00

Fusion System – Relation analysis of communication & financial transaction data

Presented by trovicor

11:30-12:00

Speeding up your investigation with existing data

Presented by trovicor

12:00-12:30

Identifying suspects of criminal events

Presented by trovicor

13:30-14:30

Virtual Human Intelligence: be inside, stealth, future and technology proof

Presented by AREA

15:00-16:00 Session A

Lawful Interception. Integrated Solution for Massive Voice and Data Gathering and Decryption

Presented by IPS

15:00-16:00 Session B

Comprehensive Solutions for Lawful Interception and Digital Surveillance

Presented by RCS

Thursday, 4 December 2014

8:30-9:30 Session A

Intelligence Analysis Platform for Monitoring Center

Presented by Telmedia Intelligence

8:30-9:30 Session B

VIBIS - Voice Identification Based Interception System

Presented by Xspec

10:30-11:00 Session A

Fusion System – Relation analysis of communication & financial

Presented by trovicor

10:30-11:30 Session B

Reduce your IP Interception cost up to 50%. Know How?

Jitendra Verma, Director Business Development, ClearTrail Technologies

11:00-11:30 Session A

Identifying suspects of criminal events

Presented by trovicor

Track 6: Social Network Monitoring and Big Data Analytics Training and Product Demonstrations

This training is only open to Law Enforcement, Public Safety and Government Intelligence Community Attendees.

Tuesday, 2 December 2014

- 8:30-9:30 **Integrating Intelligent Profiling with OSINT**
Presented by Creative Technosoft Systems
- 13:00-14:00 **Analysis and Presentation of Historical Call Detail Records: A GeoTime Case Study**
Curtis Garton, Product Manager, Oculus Info Inc
- 14:15-15:15 **Live Demonstration of OpenMIND: A True, Deep Web, End-to-End Web Intelligence Platform**
Niv Blond, Director of Sales and Marketing, 3i-MIND

Wednesday, 3 December 2014

- 9:00-10:00 **INVESTIGO-From Information to Intelligence - A Multifaceted Intelligence Analysis Platform**
Presented by RCS
- 11:30-12:30 Session **Converged Big Data Analysis and Application**
A *Presented by Sinovatio*
- 11:30-12:30 Session **Collecting Data from all parts of the Web for Intelligence (Demo)**
B *Presented by Kapow Software, a Kofax company*
- 13:30-14:30 Session **Keep your data safe, secure and in your control: A comprehensive security solution**
A *Presented by AGT*
- 13:30-14:30 Session **iWeb - New Innovation in Real-Time Interception of illegal websites & Internet traffic**
B *Presented by Expert Team PTE LTD*
- 15:00-16:00 **SIGINT, OSINT, HUMINT: Massive Data Fusion, Search & Analytics in 3 Clicks**
Presented by Advanced Systems
- 16:15-17:15 **From the Identification of Public Sentiment to the Target Profiling. A complete Open Source Intelligence solution to improve Investigations**
Presented by IPS

Thursday, 4 December 2014

- 8:30-9:30 **The New Investigator Toolbox: from Tactical to Open Source Investigations**
Presented by AREA
- 10:30-11:30 **Social Network Investigation and Forensics Platform**
Presented by Telmedia Intelligence
- 12:00-13:00 **Top 20 Open Source Tools (OSINT) Used in Cybercrime Investigations**
Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement

Track 7: Mobile Signal Intercept and Electronic Surveillance Training and Product Demonstration

This track is for Law Enforcement, Interior Security and the Government Intelligence Community who must work with cellular and mobile satellite operators regarding mobile location, electronic surveillance and intercept as well as TSCM.

This track is only open to Law Enforcement, Public Safety and Government Intelligence Community Attendees.

Tuesday, 2 December 2014

11:00-12:00 **Covert Location Intelligence - A new paradigm in intelligence gathering**
Presented by Kommlabs

Wednesday, 3 December 2014

9:00-10:00 Session A **Neosoft tactical solutions for Mobile monitoring**
Presented by NeoSoft

9:00-10:00 Session B **Precisely Locate Your Target in Half The Time**
Presented by Kommlabs

11:30-12:30 Session A **High Accuracy Location Surveillance for Challenging Border Areas**
Sridhar Kolar, VP Business Development, Polaris Wireless

11:30-12:30 Session B **Target Mobiles go LTE - How to stay in Control**
Presented by EXFO Homeland Security

13:30-14:30 Session A **3 in 1 Passive Tracker: Pinpoint the WCDMA/GSM/CDMA phone with an all in one passive tracker**
Presented by Semptian

13:30-14:30 Session B **Providence Black Catalogue**
Presented by Providence

15:00-16:00 Session A **Nomadic equipment, wearable monitoring and field Command Centre**
Presented by AREA

15:00-16:00 Session B **Commesh: Covert Audio and Video Surveillance**
Aaron Best, Sales Director, Commesh Ltd.

16:15-17:15 Session A **Crime Prevention by Combining Cell Phone Positioning and Behavioral Analysis**
Presented by Mobilaris

Thursday, 4 December 2014

8:30-9:30 **Audio, Video, GPS: Tactical Operations in a Strategic Vision**
Session A *Presented by IPS*

8:30-9:00 **Tactical and Strategic GSM-Monitoring**
Session B *Presented by SIM*

9:00-9:30 **Covert Acquisition of GSM-Data**
Session B *Presented by SIM*

10:30-11:30 **GSM/3G/LTE IMSI catcher basics. Public number detection. Mass Emergency notification. Target localization for LEAs and Search & Rescue operations.**
Session A *Presented by NeoSoft*

10:30-11:30 **TESLA: Fully Undetectable Technology, compare different solutions, Focus on Tracking and Surveillance with Data Streaming by UMTS, GPRS, WiFi, demo real installations and**
Session B *Presented by GR Sistemi*

Tuesday, 2 December 2014

Pre-Conference Seminars and Tutorials

Seminar #1

8:30-16:30

Online Social Media and Internet Investigations

Presented by *Charles Cohen, **Cohen Training and Consulting, LLC***

*Charles Cohen also holds the position of Commander, Cyber Crimes Investigative Technologies Section, **Indiana State Police, USA***

8:30-9:30: Session 1 of 6

The role of Online Social Media OSINT in Predicting and Interdicting Spree Killings: Case Studies and Analysis

This session is for criminal investigators and intelligence analysts who need to understand the impact of online social networking on how criminals communicate, train, interact with victims, and facilitate their criminality.

9:45-10:45: Session 2 of 6

OSINT and Criminal Investigations

Now that the Internet is dominated by Online Social Media, OSINT is a critical component of criminal investigations. This session will demonstrate, through case studies, how OSINT can and should be integrated into traditional criminal investigations.

11:00-12:00: Session 3 of 6

Metadata Exploitation in Criminal Investigations

This session is for investigators who need to understand social network communities along with the tools, tricks, and techniques to prevent, track, and solve crimes.

13:00-14:00: Session 4 of 6

EXIF Tags and Geolocation of Devices for Investigations and Operational Security

Current and future undercover officers must now face a world in which facial recognition and Internet caching make it possible to locate an online image posted years or decades before. There are risks posed for undercover associated with online social media and online social networking Investigations. This session presents guidelines for dealing with these risks.

14:15-15:15: Session 5 of 6

Case Studies in Metadata Vulnerability Exploitation and Facial Recognition

While there are over 300 social networking sites on the Internet, Facebook is by far the most populous, with over 800 million profiles. It has roughly the same population as the US and UK combined, making it the third largest country by population. There are over 250 million images and

170 million status updates loaded on Facebook every day. This session will cover topics including Facebook security and account settings, Facebook data retention and interaction with law enforcement, and common fraud schemes involving Facebook.

15:30-16:30: Session 6 of 6

What Investigators Need to Know about Emerging Technologies Used to Hide on the Internet

Criminal investigators and analysts need to understand how people conceal their identity on the Internet. Technology may be neutral, but the ability to hide ones identity and location on the Internet can be both a challenge and an opportunity. Various methods of hiding ones identity and location while engaged in activities on the Internet, provides an opportunity for investigators to engage in covert online research while also providing a means for criminals to engage in surreptitious communication in furtherance of nefarious activities. As technologies, such as digital device fingerprinting, emerge as ways to attribute identity this becomes a topic about which every investigator and analyst may become familiar.

Seminar #2 8:30-16:30

Understanding ISS Technologies and Products Deployed in Telecommunications Networks and Monitoring Centers for Law Enforcement and Intelligence Analysts

Presented by: *Dr. Jerry Lucas, President, TeleStrategies*

This one day pre-conference seminar covers the spectrum of ISS Technologies and Products deployed in today's fixed wire, mobile wireless and Internet Service Provider networks and LEA Monitoring and Intelligence Gathering Centers. This all day seminar is ideal for those law enforcement, public safety and intelligence analysts who need an understanding of the ISS technologies to be discussed in the conference sessions and the ISS products displayed at the exhibit hall as well as an understanding of the buzz words and jargon used by telecom operator engineers and their vendors.

08:30-10:45

Introduction to Telecom Infrastructure, Interception and Related ISS Products

What do LEAs need to know about telecommunications networks infrastructure, basic LI elements (access, delivery and collection function), LEA Monitoring Center Functions and where are ISS products deployed for monitoring and intercept.

Understanding ISS:

Why Understanding Telecom Infrastructure is Important for Law Enforcement and Intelligence Analysts

Basic Telecom Building Blocks:

Circuit vs. Soft IP Switching, Signaling (SS7, ISDN, DTMF, etc.), fiber optics (SDH and SONET), Broadband Access (DSL, Cable Modems, Wi-Fi etc.), IP Core Technologies (Routing, ATM, MPLS, etc.) and Network Elements for Intercept.

Telco Back Office Systems:

Billing Systems, Mediation Services for Capturing Call Detail Records and LEA Intercept Request Processing.

Lawful Interception Architectures:

Probes (active and passive), Optical Layer Intercept at 10, 40 and 100 GBPS, Mediation and Data Retention Architectures, CALEA Pen Register and Trap & Trace, LEA Monitoring Center Functions and ISS Products Deployed in Fixed Wire Network Infrastructure.

Typical US DEA Funded LI Systems:

LIMS, T2S2, Warrant Processing, Data Logs, Capacity Requirement (e.g. Targets, Handoff Circuit Capacity, etc.) Central America Project Funding and Enterprise Hardware/Software Requirements

Legal Intercept Options:

What must telecom operators provide with a served subpoenas, Search Warrant, CALEA-Title III, National Security Letter and FISA Warrant.

11:00-14:00

Understanding Mobile Wireless Infrastructure, Interception and Related ISS Products

Infrastructure basics, back office infrastructure, IM, data and where are ISS products deployed for monitoring and intercept.

Types of Wireless Network:

Differences among Network Operators, MUNO's, WiFi, WiMAX, Microwave, Satellite, Femtocells and NFC Interfacing.

Mobile Network Infrastructure:

Subsystems (cell sites, sector antennas, back hall, processors at towers, MSO special features (HLR, VLR, etc.) and PSTN Interconnect.

Cellular Network Generations:

Infrastructure Difference Among GSM, GPSS, EDGE, HSPA, North American CDMA, W-CDMA and LTE (CSFB vs. IMS Based) and Difference in Data Service Support.

Smartphones:

Functional Differences between 3G/4G Smartphones and 2G Phones, SMS messaging vs. iPhone text messages regarding intercept and 3G vs. LTE data services capabilities.

Cell Phone CDR's:

What records do cellular operators obtain when the phone is on, what's in a CDR when phone call is initiated and other forensic data of value to LEA's.

Cell Phone Tracking Options:

Cellular Operator Tracking Services available to LEA's, Target Pinging, Location technologies (GPS

is National Based vs. RF Spectrum Mapping, GSM Surveillance, A-GSM intercept, WiFi Tracking, IMSI/IMEI Catchers, Spyware and more.

Smartphone Services to Avoid Tracking:

WHATSAPP, TIGER Text, WICKR, VIBER, GroupMe and more.

ISS Intercept Product Options:

Electronics Surveillance (audio, video and GPS), Location Based Mediation Products, Smartphone IT Intrusion and Cellular CDR data mining, Geocoded Photo Metadata, EXIF tags, Special Smartphone Services for Geolocation (Creepy, Instagram, Foursquare, VIBE and more).

14:15-16:30

Understanding the Internet, Interception and Related ISS Products

What Investigators Have To Know about IP call Identifying Information, Investigations Involving E-Mail, Facebook, Twitter, Skype, Instant Messaging, Chat Rooms and what can be done to address Internet intercept deploying ISS infrastructure and where are ISS products deployed for monitoring and intercept.

IP Basics:

Why Understanding IP Layering Model, TCP/IP and UDP is important for LEA's and the IC Community, IP addresses (IPv4 vs. IPv6), static vs. dynamic addresses and more.

Internet Players:

The managers (ICANN, IANS and IETF), NSPs vs. ISPs vs. CDNs, How the Internet Players exchange IP Traffic, Private vs. Public peering and IXPs.

ISP Infrastructure:

RAS, RADIUS, DHCP and DNS and why these servers are important to understand.

VoIP Options:

Types of VoIP Services, PSTN interconnect, Gateway Based (Vonage), P2P (Skype & VIBER), Softswitches, SIP and IMS.

E-mail Services:

Client Based E-mail vs. Webmail. What's different about E-mail, SMS, WEB 2.0, HTTPS, HTTPS 2.0, Smartphone messaging and Social Network messages.

Social Network Metadata:

From Tweets, Facebook, E-mail and Smartphones.

Deep Packet Inspection:

What's DPI, Where do telecoms deploy DPI and Where does the Intelligence Community request DPI intercept.

Defeating Encryption:

Encryption options, Public Key Encryption, TOR, Third Party Services Available (Wickr), Encryption Products and how to defeat encryption (Spyware, Remotely Loaded Programs, IT Intrusion and Man-In-The-Middle Attacks)

ISS Products for Intelligence Gathering:

OSINT, Big Data Analytics, Speaker Recognition, Facial Recognition, IP Mediation Devices and Monitoring Centers.

Seminar #3

8:30-16:30

Practitioners Guide to Internet Investigations

Presented by: *Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement, **UK Police***

The aim of this 1 day seminar is to take the attendees from the basics of understanding the internet, how to find data, through to a full understanding of best practice of an internet investigator, having awareness and knowledge of all the tools available to achieve this.

This is exclusively Law Enforcement only, as Practical examples, covert and investigative methods will be given throughout the seminar.

8:30-9:30

The World Wide Web and the Internet

- How it works. Why it works. How data traffic leaves a trace ;
- What the internet is; what is an IP and what protocols are used (TCP/IP)
- IPv4 and IPv6 – understanding the changes
- mirror servers use and value
- Tracking and evaluating data

9:45-10:45

Recognizing Traffic Data

- A practitioner's guide to what data is available. How to harvest and analyze it.
- Best practice to identify suspects and build profiles.
- Data collection and interrogation
- IP usage, exploitation and dynamics; IP plotting and analysis how to look for suspect mistakes and exploit them (where they show their id)
- Dynamic approaches to identifying suspects through internet profiles
- What investigators get from tech and service providers, and how to analyze it
- What to ask for with current legislation to achieve best results
- SPOC best practice.
- ISP/ CSP capabilities and opportunities.

11:00-12:00

WIFI and Mobile Data

- A practitioner's look at Wi-Fi, attribution, cell site data, GPRS location services and technology. How an investigator can track devices, attribute suspects locations, devices and movement.
- Dynamic live time tracing
- Geo location services and uses
- Surveillance without DSA and authority

13:00-14:00

Emerging Technologies, Masking Tech and Tools

- How suspects are using emerging and new technologies.
- An introduction to where technology is going, and how Law enforcement can use this to our advantages.
- Darknet, (Deepweb) and IRC use
- VOIP, Skype
- Advanced data sniffing and profile building
- TOR systems, applications and ways to coax offenders out of the system.

14:15-15:15

Advanced Techniques in Tracing Suspects

- Using innovative and dynamic methods to trace offenders.
- tricks used by suspects and how to combat them
- Covert internet investigations
- Proxy servers and hiding.
- managing collateral intrusion
- Reverse and social engineering
- Thinking outside the box
- Possible missed opportunities
- Profile building and manhunts

15:30-16:30

Open Source Intelligence Training (OSINT)

- An in depth look at what tools are available; how to use them, and practical applications.
- safety online when open sourcing

- open source training and awareness basics
- Trace suspects using available tools
- How to identify leads in investigations and data from ISP
- Internet tools to assist in building online profiles on suspects
- A run through of my website dedicated to online tracing tools and how best to use it (LEA ONLY)
- Reverse engineering and social engineering