-
-
-
-
-
-
-
-

ISS World Americas is the world's largest gathering of North American, Caribbean and Latin American law enforcement, intelligence, homeland security analysts and telecom operators responsible for lawful interception, electronic investigations and network intelligence gathering.

ISS World's education programs present the methodologies and tools to bridge the chasms of lawful intercept data gathering to information creation to investigator knowledge to actionable intelligence.

ISS World Americas - Conference Agenda at a Glance
October 11-13, 2011

Tuesday, October 11, 2011

Pre-Conference Training Seminars

8:30-4:30

Online Social Media and Internet Investigations (Six One Hour Sessions)

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

Charles Cohen also holds the position of Commander, Special Investigations and Criminal Intelligence, **Indiana State Police, USA**

8:30-12:00

Understanding Telecommunications and ISS Technologies for LEA Investigators and Intelligence Analysts (Three One Hour Sessions)

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

1:00-4:30

Basics of Internet Intercept for Law Enforcement and Intelligence Analysts (Three One Hour Sessions)

Matthew Lucas (Ph.D, Computer Science), Vice President, ***TeleStrategies***

1:00-4:30

Visual Analytics For Detecting Criminal Patterns

Chris Westphal, CEO, ***Visual Analytics***

8:30-4:30

Implementation of a Tactical Communications Analytical Unit in Your Agency (Six One Hour Sessions)

Robert Lottero, President, ***NTI Law Enforcement Services***

8:30-4:30

Cell Phone Intelligence Training

Presented By Breck McDaniel, President, ***Geocell, LLC****. Breck also holds the position of Sergeant Houston Police Department.*

8:30-2:00

WIRETAPPING understanding the basics

James Deater, President, ***T3TECHSYSTEMS***

8:30-10:45

Introduction to Physical Recovery for Digital Forensic and Intelligence Labs

Alvaro Alexander Soto, Director of Digital Forensics & Security Laboratory, ***Asoto Technology Group***

11:00-12:00

Advanced Digital Forensic Process and tools for Law Enforcement and Intelligence Analysts

Alvaro Alexander Soto, Director of Digital Forensics & Security Laboratory, ***Asoto Technology Group***

1:00-2:00

The Basics of Weaponized Information

Stephen Arnold, Managing Partner, ***ArnoldIT.com***

2:15-3:15

Cell Phone Calls and Cell Tower Records for Investigators

Brent Bailey, ***Cellular Data Resources***

3:30-4:30

Cloud Lawful Interception and Data Retention

Tony Rutkowski, VP, ***Yaana Technology***

(Full Pre-Conference Seminar Agenda Appears After Track 7)

Wednesday, October 12, 2011

Welcoming Remarks

8:15-8:30 *Tatiana Lucas, ISS World Program Director,* ***TeleStrategies***

ISS World Keynote Addresses

8:30-9:00 **Top Ten Internet Challenges Facing Law Enforcement and the Intelligence Community**
Dr. Jerry Lucas, President, ***TeleStrategies***

9:00-9:30 **Online OSINT: Observation & Infiltration**
Charles Cohen, ***Cohen Training and Consulting, LCC***
Charles also holds the position of ***Commander, Special Investigation and Criminal Intelligence, Indiana State Police***

9:30-10:00 **What Intelligence Analysts Need to Know about Search Engine Results Manipulation**
Stephen Arnold, Managing Partner, ***ArnoldIT.com***

ISS World Americas Exhibits

Wednesday, October 12 - 10:00 AM - 6:00PM

Thursday, October 13 - 9:30 AM - 12:30 PM

Track 1: ISS for Lawful Interception

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

Wednesday, October 12, 2011

11:00-12:00	**LI for New IP Services "Best Practices" Guru Panel** *Rudolf Winschuh, Business Development Manager,* ***Utimaco LIMS*** *Bert Hubert, Lawful Interception Specialist,* ***Fox-IT*** *Chris MacFarlane, President,* ***ETI Connect*** *Aubrey Merchant-Dest, Senior Systems Engineer,* ***Qosmos*** *Dr. Elan Amir, President and CEO,* ***Bivio Networks*** *Jim Donnelly, VP of Sales for the Americas,* ***Glimmerglass Networks*** *Dan Pocek, CEO,* ***NetQuest*** *Dr. Cemal Dikmen, CTO,* ***SS8*** *O.J. Johnston, Director of Government Solutions,* ***ONPATH***
1:30-2:00 Session A	**Interception at 100Gbps and beyond** *Aubrey Merchant-Dest, Senior Systems Engineer,* ***Qosmos***
1:30-2:00 Session B	**Mobile Location Tracking that is based on a Integration of an in network GMLC and Tactical Cellular Location Direction Finders** *Elan Sharon,* ***Septier***

2:00-2:30 Session A	**Reducing the Cost of Managing Warrents and Subpoenas** *Ray Green,* ***Focus Data Services***
2:00-2:30 Session B	**Manage the flood** *Jeff Zindel, Vice President, Marketing and Product Management,* ***Glimmerglass Networks***
3:00-3:30 Session A	**Automatic Discovery and Interception of International Leased Line Services** *Jess Price, VP Sales and Marketing,* ***NetQuest Corporation***
3:00-3:30 Session B	**LI in Clouds - Challenges & Possible Opportunities for Providers & LEAs** *Rudolf Winschuh, Business Development Manager,* ***Utimaco LIMS***
3:30-4:00 Session A	**Challenges of Webmail Interception and Analysis** *Cemal Dikmen, CTO,* ***SS8***
3:30-4:00 Session B	**From Gigabits to Terabits: Why you want to work smarter and not harder** *Chris MacFarlane, President,* ***ETI Connect***
4:30-5:00 Session A	**Why Terabits is not a Challenge** ***ETI Group,*** *speaker to be announced*
4:30-5:00 Session B	**Cutting Edge Mobile Initiatives and Wireless Network Transmission Technologies for Law Enforcement and Government Applications** *Gary Hatch, CEO,* ***ATCi***

Thursday, October 13, 2011

9:00-9:30	**Lawful Intercept: From Copper to Fiber and Back** OJ Johnston, Director of Government Solutions, **ONPATH Technologies**
10:30-11:00	**3G to LTE: Evolution and Changes** *Luis Alves, Senior Director, Business Development,* ***Aqsacom***
11:00-11:30	**Connecting the Dots: Turning Mobile Data into Actionable Intelligence** *Elan Amir, President and CEO,* ***Bivio Networks***
1:00-1:30	**Paradigm Shifts** *James A. Donnelly, Vice President of Sales,* ***Glimmerglass Networks***

1:30-2:00	**IPv6 Migration Strategies must Include LI - Forgetting this can be very costly** *David Cooke, Area Sales Manager,* ***ETI Connect***

Track 2: ISS for Criminal Investigations

This track is for Law Enforcement, Intelligence and Cyber Security Analysts who have investigation responsibilities associated with telecommunications networks.

Wednesday, October 12, 2011

11:00-11:30	**Exploiting Computer and Mobile Vulnerabilities for Electronic Surveillance** *Chaouki Bekrar, CEO & Director of Vulnerability Research,* ***Vupen Security***
11:30-12:00 Session A	**Empowering Cyber Intelligence Operations: a stealth, spyware-like software to attack, infect and collect evidence from Computers and Smartphones** *David Vincenzetti, Partner,* ***Hacking Team***
11:30-12:00 Session B	**IP Based Investigations - Not Only for Forensics** *Jenny Grinberg, Product Manager,* ***Verint Systems***
1:30-2:00	**Countermeasures to Identify Cybercriminals Hiding on the Internet** *Lance Cottrell, CTO,* ***Ntrepid***
2:00-2:30	**Needles in the haystack: Applying lessons learned in Digital Forensics to the challenges in LI** *Dirk Peeters, VP of International Business Development,* ***Fox-IT***
3:00-3:30	**"Fibre Analyzer" A view at fibre and broadband links** ***VASTech*** *Engineering*
3:30-4:00	**Access Switching - Identifying the Needle in the 10/40/100G Haystack** *Sharon Besser, VP of Technology,* ***Net Optics***
4:30-5:00	**A comprehensive solution for operational, tactical and strategic Communication Intelligence** *Steve Hodges, VP Sales & Business Development, North America,* ***Agnitio***

Thursday, October 13, 2011

8:30-9:00	**How IPv6 Improves Investigators' Work** ***ETI Group,*** *speaker to be announced*
9:00-9:30	**Speaker Identification for Forensic and Criminal Investigation, Helping the Law Enforcement Agencies Mission** *Antonio Moreno, Technical Sales Director,* ***Agnitio***
10:30-11:00	**The Distinct Roles and Values of an End-to-End IP Intercept Solutions** *Derek Granath, VP, Product Line Management,* ***SS8***
11:00-11:30	**The Use of Consumer Surveillance Technologies in Cell Phone Surveillance** *Tim Phipps,* ***Cambridge Consultants***
11:30-12:00	**Handheld Tools for Cell Phone Direction Finding and Location** *Scott N. Schober, President & CEO,* ***Berkeley Varitronics Systems***

Track 3: ISS for Data Retention and Regulatory Compliance

This track is for Telecom Operators and Law Enforcement, Intelligence and Defense Analysts who are responsible for Call Data Retention and Data Handoff

Wednesday, October 12, 2011

1:30-2:00	**SMS, the forgotten source of intelligence!** *Dirk Schrader, Sales Director,* ***Utimaco LIMS***
3:00-3:30	**Context-Based Data Retention using Multi-Source Collection & Correlation** *Joel Ebrahimi, Solutions Engineer****, Bivio Networks***
3:30-4:00	**The Next Generation in Handover Format Conversion and Interception Data Buffering** *Bob Brandt, Product Manager Replay,* ***Fox-IT***

4:30-5:00	**Metadata Extraction and Retention for IP Applications** *Derek Granath, VP Product Line Management, **SS8***
5:00-5:30	**Overview: Data Retention in Europe - Current status from various aspects** *Ramon Mendez, Director Sales, **Utimaco LIMS***

Thursday, October 13, 2011

10:30-11:30	**New Congressional Proposals on Data Retention and Privacy. What's the Impact on Telecom Operators** *Joel M. Margolis, Senior Regulatory Counsel, **Subsentio*** *Todd P. McDermott, Vice President, **Verint Systems***

Track 4: DPI for Lawful Interception and Cyber Security

This track is for telecom operators, law enforcement, intelligence analysts or just about anyone who has to understand Deep Packet Inspection (DPI) technologies, product availability, applications and legal issues facing telecom operators who deploy DPI infrastructure

Wednesday, October 12, 2011

11:30-12:00	**You Can't Catch What You Can't See: Traffic Visibility-The Cornerstone of Lawful Intercept** *Yury German, CISSP, GCIH, Senior Security Architect, **Gigamon***
1:30-2:30	**Best DPI Deployment Practices for LI, Network Security and Traffic Management Guru Panel** *Mike Coward, Chief Technology Officer & Co-Founder, **Continuous Computing*** *Jerome Tollet, Chief Technology Officer, **Qosmos*** *Dr. Elan Amir, President and CEO, **Bivio Networks*** *Daniel Proch, Director of Product Management, **Netronome*** *Jason Richards, CEO, **Vineyard Networks***

3:00-3:30	**DPI at 100G: System Architectures and Real World Deployments** *Mike Coward, CTO & co-founder,* ***Continuous Computing***
3:30-4:00	**Scaling DPI, LI and Network Security Solutions to 40Gbps and Beyond** *Daniel Proch, Director of Product Management,* ***Netronome***
4:30-5:00	**Dealing with an ever changing sea of Application Protocols** *Jerome Tollet, CTO,* ***Qosmos***

Thursday, October 13, 2011

8:30-9:00	**Effective Use of DPI-Enabled Technology for Security, Monitoring and Control** *Joel Ebrahimi, Solutions Engineer,* ***Bivio Networks***
9:00-9:30	**Understanding Passive Monitoring Techniques for Mass Intercept and Mass Location Tracking** *Ray Hutton,* ***Telesoft Technologies***
10:30-11:00	**Open Networking in Lawful Interception** *Robert Lin, Director of Sales,* ***Simena***
11:00-11:30	**Scalable Extraction, Aggregation, and Response to Network Intelligence** *Hari Kosaraju,* ***Mantaro Networks***
11:30-12:00	**Making L7 Classification and DPI Easy** *Jason Richards, CEO,* ***Vineyard Networks***
1:00-1:30	**Interception and Intelligence Gathering - Impact of Growing Bandwidth and New IP Applications** *Derek Granath, VP, Product Line Management,* ***SS8***

Track 5: ISS for Intelligence Gathering and Analysis

This track is for intelligence analysis and law enforcemet agents who have to "connect the dots" between people, places and other entitites by searching through various data sources from data text to information on behavior patterns.

Wednesday, October 12, 2011

11:00-11:30	**Who, What, When, Where and How: Semantics Helps Connect the Dots** *GianPiero Oggero, Director Strategic Accounts, Intelligence Division,* ***Expert System*** *Andrea Melegari, COO, Intelligence Division,* ***Expert System***
11:30-12:00	**Anatomy of a Social Network: Finding Hidden Connections and True Influencers in Target Data** *Mat Mathews, Director,* ***Ntrepid***
1:30-2:00	**Deep Semantic vs. Keyword and Shallow Linguistic: A New Approach for Supporting Exploitation** *Rita Joseph, Vice President, Federal,* ***Expert System***
2:00-2:30	**Detecting new threats and suspects in e-mails, SMS, Chat Multilingual Conversations** *Bastien Hillen,* ***Scan & Target***

Track 6: OSINT, Metadata and Visual Analytics for Intelligence Gathering

This track is for intelligence analysts who must gather on-line intelligence by deploying Visual Analytics, Speech Recognition, Web Intelligence, Data Mining and OSINT programs.

Wednesday, October 12, 2011

11:00-11:30	**Lessons learned from the top 3 U.S. government OSINT programs** *Andrew Lasko, PMP, Technical Alliance Manager,* ***Kapow Software***
11:30-12:00	**Empowering Cyber Intelligence Operations: a stealth, spyware-like software to attack, infect and collect evidence form computers and smartphones** *David Vincenzetti, Partner,* ***Hacking Team***

1:30-2:00	**Lawful Interception in Virtual Environments** *Ran Nahmias, Director of Cloud Solutions, **Net Optics***
2:00-2:30	**Mass IP Metadata Analysis-Challenges and Solutions** *Cemal Dikmen, CTO, **SS8***
3:00-3:30	**Gathering Open Source Intelligence Anonymously** *Lance Cottrell, CTO, **Ntrepid***
3:30-4:00	**The Key to OSINT - Finding and harvesting "topic specific" content from the Deep Web** *Steve Pederson, CEO, **BrightPlanet Corporation***
4:30-5:00	**Modern Global Cyber Monitoring Techniques** *Victor Oppleman, President, **Packet Forensics***

Thursday, October 13, 2011

9:00-9:30	**Evaluation and Intelligence Fusion in Technical Reconnaissance** *Professor Klaus Ehrenfried Schmidt, **MEDAV GmbH***
10:30-11:00	**Boosting Monitoring Centers with IP Metadata** *Jerome Tollet, CTO, **Qosmos***
11:00-11:30	**Human Movement Analysis: Visual Analysis of Movement Patterns Based on Communication Records** *Curtis Garton, Product Manager, **Oculus Info***
11:30-12:00	**Gaining Meaningful Intelligence from Massive Volumes of Real Time Voice Intercepts** *Marlin Nelson, Director of Sales and Business Development, **NICE***

Track 7: LEA, Intelligence and Defense Analyst Training and Product Demonstration Track

This training and product demonstration track is open only to Law Enforcement, Intelligence, Defense Analysts and other Government Executives.

Wednesday, October 12, 2011

9:00-10:00 Session A	**"Satellite Signal Analyzer" Discover de Sky. Product Presentation: Satellite Signal Analyzer Generation** *Fabrizio Diantina, Regional Manager for Americas,* ***VASTech*** *Roland Jones, Sales Manager,* ***VASTech***
9:00-10:00 Session B	**High Performance Computing and Storage solutions, for laboratories and field operations of Law Enforcement and Intelligence** *Alvaro Alexander Soto, Director, Digital Forensics & Security Laboratory,* ***Asoto Technology Group***
11:00-12:00 Session A	**BS3, the key speaker spotting tool helping Intelligence Analytics** ***Agnitio*** *Speaker to be Announced*
11:00-12:00 Session B	**Efficient Analysis and Case management Tools - the prerequisites for successful LI, product demonstration** *James Hostelley, Client Solutions Coordinator,* ***ETI Connect***
11:00-12:00 Session C	**Tactical Intercepts in High-Stakes Environments** *Victor Oppleman, President,* ***Packet Forensics***
1:30-2:30 Session A	**Government IT Intrusion: Applied Hacking Techniques Used by Government Agencies** *MJM, IT Intrusion Expert,* ***Gamma Group***
1:30-2:30 Session B	**Tools for Handling IP Based Investigations** *Jenny Grinberg, Product Manager,* ***Verint Systems***
3:00-4:00 Session A	**Remote Control System 7: The ultimate cyber-intelligence solution for covertly monitoring Computers and Smartphones** *Marco Valleri, Senior Security Engineer,* ***Hacking Team*** *Alberto Ornaghi, Senior Security Engineer,* ***Hacking Team***
3:00-4:00 Session B	**Social Network Analysis Techniques for Analyzing Intercepted IP Communications** *Corey Lanum, SE,* ***SS8*** *& Derek Granath, VP Product Line Management,* ***SS8***
4:30-5:30 Session A	**VUPEN Vulnerability Research and Sophisticated Exploits for Offensive Security** *Chaouki Bekrar, CEO & Director of Vulnerability Research,* ***VUPEN Security***
4:30-5:30 Session B	**Multi-Source Data Correlation for Intelligent Retention & Action** *Joel Ebrahimi, Solutions Engineer,* ***Bivio Networks***

Thursday, October 13, 2011

8:30-9:30 Session A	**Offensive IT Intelligence and Information Gathering Portfolio-An Operational Overview** *MJM, IT Intrusion Expert,* ***Gamma Group***
8:30-9:30 Session B	**FoxReplay Analyst 3.0 'Blanford' Product Demonstration** *Bob Brandt, Product Manager Replay,* ***Fox-IT***
8:30-9:30 Session C	**Extracting Intelligence & Evidence from Accurate Location Technologies** *Yochai Corem, Director of Product Marketing,* ***Verint Systems***
10:30-11:30 Session A	**Remote Control System 7: an in-depth, live demonstration of infection vectors and attack techniques for targeting Computers and Smartphones!** *Marco Valleri, Senior Security Engineer,* ***Hacking Team*** *Alberto Ornaghi, Senior Security Engineer,* ***Hacking Team***
10:30-11:30 Session B	**ION Secure Virtual Desktop: Conducting Safe and Non-attributable Online Research and Investigation** *Lance Cottrell, CTO,* ***Ntrepid***
10:30-11:30 Session C	**Manage the flood** *Joon Choi, Director of Product Management,* ***Glimmerglass Networks***
11:30-12:30 Session C	**Intelligence Driven Transformation Management** *Matan Efrima, Intelligence Methodology Expert,* ***Verint Systems***
1:00-2:00 Session A	**Off-Air Cellular and Satellite Interception-Hybrid Solution** *Amir Barel, VP,* ***Verint Systems***

Pre-Conference Seminars and Tutorials

Pre-Conference Training Seminars

Tuesday, October 11, 2011

Online Social Media and Internet Investigations (Six One Hour Sessions)

Presented By

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

Charles Cohen also holds the position of Commander, Special Investigations and Criminal Intelligence, **Indiana State Police, USA**

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

What Investigators & Analysts Need to Know about Online Social Media.

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

Successful Use of Online Social Media 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.

1:00-2:00: Session 4 of 6

Counterintelligence & Liabilities Involving Online Social Media

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.

2:15-3:15: Session 5 of 6

What Investigators Need to Know about Hiding 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 activates 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 my become familiar.

3:30-4:30: Session 6 of 6

Cyberspace Money Laundering: Tools, Tricks & Techniques

Today, every investigator and analyst must at least understand the basics of the Internet online monetary transactions in order to be effective. This session addresses eCash to online virtual stored value cards and from virtual currencies to mobile payment systems. The Internet is a panacea for the active or aspiring entrepreneurial criminal.

Understanding Telecommunications Technologies and ISS for LEA Investigators and Intelligence Analysts (Three One Hour Sessions)

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

8:30-9:30

Understanding Wireline Telecom Infrastructure, Interception and Related ISS Products

What do LEAs need to know about the public switched telecommunications networks, circuit switching, fiber optics, SS7, SDH, DSL, billing systems and call detail records, standards overview for lawful intercept, basic LI elements (access, delivery and collection function), call information and call content data collection, SS7 probes and relevant telecom network elements. Circuit Switching vs. VoIP, SIP, SoftSwitches, Gateways, VoIP over Broadband, DSLAM's and PSTN Interconnection.

9:45-10:45

Understanding Mobile Wireless Infrastructure, Interception and Related ISS Products

Infrastructure basics (GSM, GPRS, EDGE, UMTS, HSPA and LTE), Wi-Fi, WiMax and Femtocells, How a cellular call is processed, back office infrastructure, HLR, VLR, Backhaul and PSTN interconnection, data services, SMS, MMS, EM, data services, fixed mobile convergence and IMS. The basics of mobile wireless technologies, A-GPS, AOA, TDOA, U-TDOA, WLS and location accuracy. Transforming cell records and location data into actionable intelligence, Smart Phone intercept and wireless provider business model, Apple iPhone, Google Android and LTE Challenges.

11:00-12:00

Understanding the Internet, Interception and Related ISS Products

What Investigators Have To Know about IP call Identifying Information, Radius, DHCP, DNS, etc. and Tracking an Internet Address to a Source, Investigations Involving E-Mail, Websites, Skype, Instant Messaging, Chat Rooms and Message Boards, IMS, P2P Networks and Deep Packet Inspection and what can be done to address Internet intercept deploying ISS infrastructure, what can't be done without new legislation and future challenges law enforcement and the intelligence community faces.

1:00-4:30

Basics of Internet Intercept for Law Enforcement and Intelligence Analysts (Three One Hour Sessions)

Matthew Lucas (Ph.D, Computer Science), VP, ***TeleStrategies***

1:00-2:00

Understanding Web 2.0, IM, P2P and Social Networking Messaging (Facebook, Twitter, ect.)

Learn about advanced IP applications, including: social networking communications models, web2.0 apps, computing models and intercept options.

2:15-3:15

Understanding TCP/IP for Packet Traffic Analysis

Learn the basics/fundamentals of IP network, including: key equipment components, network access types, service provider infrastructure, IP protocol basics, TCP protocols and applications.

3:30-4:30

Understanding DPI for LEAs, Intelligence Analysts and Telecom Operators

Learn packet intercept by example, including: intercept options, probe types, packet capture, packet analysis and application protocol decoding.

1:00-4:30

Visual Analytics For Detecting Criminal Patterns (Three One Hour Sessions)

This presentation addresses the use of various visualization and representation techniques for understanding a variety of domains ranging from financial crimes and money laundering to narcotics-trafficking and counter-terrorism. Much of the content presented is based on Mr. Westphal's recent book, "Data Mining for Intelligence, Fraud & Criminal Detection: Advanced Analytics & Information Sharing Technologies" (CRC Press, December 2008).

Chris Westphal, CEO, ***Visual Analytics***

1:00-2:00

Overview of Analytical Process Using Visualization

2:15-3:15

Data Quality and Integration Approaches Pros/Cons

3:30-4:30

Real World Patterns (e.g. Money Laundering, Fraud, Crime)

8:30-4:30

Implementation of a Tactical Communications Analytical Unit in Your Agency (Six One Hour Sessions)

Robert Lottero, President, ***NTI Law Enforcement Services***

A detailed review of the equipment, hardware, software, analytical/reporting techniques, and concepts necessary to put into operation an analytical unit that can exploit communications records (Landline, cell, VoIP, Satphone, Prepaid calling cards, and emails) in support of criminal and national security investigations

Function of a Tactical Communications Analysis Unit (TCAU)

Acquire real time and historical communications records and perform appropriate analyses to determine relationships, hierarchy, and organizational structure of co-conspirators and identify individual involvement in criminal and/or terrorist activities. Integrate the results of communications analysis with other intelligence information (activities, financial transaction, surveillance, etc.) collected during the investigative process to generate tactical leads that support the ongoing investigative process.

8:30-9:30

Acquisition of communications records: What to get (real time & historical). How much to get. Validating and understanding records received

9:45-10:45

Preparing and formatting communications records for computer analysis.

Hardware and software to pre-process raw communications records for electronic storage

11:00-12:00

Understanding basic and advanced analytical concepts.

Enhancing the results of basic contact communications analysis (frequency, common call, etc.). Advanced communications temporal analytical theory.

1:00-2:00

Understanding the functionality you'll need in database & analytical software. Functionality needed to support your operation. Database storage to properly hold communications and related records. Selecting advanced analytical software to perform contact and temporal direct and implied analysis of those records

2:00-3:00

Presentation of findings – Interpreting the results of computerized analysis of communications records and generating tactical leads. A new approach to writing and presenting analytical reports

15:30-16:30

Building the TCAU – Staffing- Choosing the right people and training. Working with vendors. Putting analytical workflow and operational procedures in place.

8:30-4:30

Cell Phone Intelligence Training (Seven 50 Minute Sessions)

Presented By Breck McDaniel, President, ***Geocell, LLC****. Breck also holds the position of Sergeant Houston Police Department.*

This one day training course will be a thorough introduction to the investigative options that are available to government officials when it comes to cellular telephones. the presentation will cover what data is available, what is "communications intelligence", why use the data, where is the data held, and, how is the data commonly used by law enforcement. The presentation will detail the available categories of information, including forensically available, historically available from companies, and, the surveillance options that exist. Coverage will also discuss important legal considerations, analysis of the data including geographic capabilities, and, tricks and challenges. The presentation will end with important courtroom presentation considerations regarding this valuable data.

8:30-9:30

Introduction; Course Goals and Outline

What is communications data and communications intelligence?; why use the data?; where is the data held?; how do we use the data?; start thinking proactively; assess the needs to access communications data in your cases and balance against other responsibilities; and, why we can't keep ignoring this extremely valuable data!

9:45-10:45

How can you use the data in your cases?

Including activation and subscriber information, payment information, communications("call") detail records (CDRs) (with, and without, geographic data), stored communications such as the content of text messages, voicemails, and emails, and, surveillance options: traps and traces/pen registers (CALEA deliveries), geolocations, cell phone locations, "target developments", communications intercepts ("wiretaps"), and, the prepaid cell phone myth, including what are Mobile Virtual Network Operators (MVNOs)?

11:00-12:00

Legal Block:

Manual searches (physcial forensics); what legal situations and what legal demands get you what?; what legal demands can you use: physical device consent, physical device search warrants, consent for records, subpoenas, court orders, and search warrants for the carriers?' what about accessing stored electronic communications?; "emergency requests", preservation requests; legal demand templates; "boilerplate"; typically two legal burdens (legal threshold); "stepping-stone approach".

1:00-2:00

Introduction to Physical Forensics Considerations Regarding:

Cell Phones, Computer, and Digital Devices, including evidence collection considerations (especially for first responders), fast verse thorough forensic approaches; and, what data is available forensically?

2:15-3:15

Introduction to Law Enforcement Surveillance Capabilities Regarding:

Cell phones, Landlines, and the Internet, including, traps and traces/pen registers [Communications Assistance for Law Enforcement Act (CALEA) deliveries], geolocations, field cell phone locations, "target developments", and communications intercepts ("wiretaps"); and, capabilities that are required to conduct real-time surveillances, including legal issues, hardware and software, financial issues, manpower, data connections, etc.

3:30-4:30

Introduction to Courtroom Presentations of Cell Phone Data; Where is Electronic Communications Data use by Law Enforcement Headed?; Future challenges and future benefits; where can you get more information and training?; suggestions about developint your own resources and important resources considerations for management, including financial, manpower, hardware, software, key legal concerns, and lobbying your own agency for support; legislative considerations; course evaluations; certificates; and, closing.

8:30-4:30

WIRETAPPING understanding the basics (Six One Hour Sessions)

James Deater, President, ***T3TECHSYSTEMS*** *James Deater also holds the position of Sergeant, Maryland State Police.*

This one day course will be an introduction and overview of wiretap investigations. Wiretap-Title III investigations are a highly advanced investigative technique/tool used by law enforcement and intelligence agencies throughout the United States and abroad. This extremely valuable tool is often not used due to misconceptions and lack of understanding. This one-day course will demonstrate the basics for law enforcement/intelligence agencies to overcome the fears of conducting a wiretap investigation and show how beneficial this tool can be. The class will include current intercept technologies and brief demonstration, the pre-wiretap investigation needed to obtain an interception order, the actual wiretap investigation during the wire, and how to properly manage and run the wiretap room.

8:30-9:30

Wiretap Technologies

What interception systems are available to government agencies and their benefits. A brief demonstration will be given of the Sytech ADACS4 interception system to give students a real-life glimpse of an operational system.

9:45-10:45

Pre-Wire Tap Investigation

This block of instruction will explain to the student eh necessary requirements that are needed prior to authoring the wiretap. Items such as PEN registers, surveillance, exhaustion and de-confliction will be addressed. Teh Affidavit, Application for Exparte, Exparte Order (long and short) and minimization will also be explained. Students will be provided with examples on CD.

11:00-12:00

Detailed Explanation of PEN Analysis

Needed for wiretaps and how to do a PEN analysis without expensive software programs

1:00-2:00

Case Management, Notifications, 10 Day report, FBI-LEO Virtual Command Center VCC

How to integrate the VCC into your wire investigation.

2:15-3:15

The Actual Wiretap Investigation

Once you are "online", what to expect, how to manage the information flow, how to "tickle" the wire, how to properly conduct "wall-off" operations and manage the flow of information.

3:30-4:30

Key Consideration for Setup and Layout of a Wire Room (temporary or permanent)

Class is only open to law enforcement, intelligence analysts and government support personnel only. Due to the sensitive and confidential nature of the information presented ID may be checked prior to class room access.

8:30-10:45

Introduction to Physical Recovery for Digital Forensic and Intelligence Labs

Alvaro Alexander Soto, Director of Digital Forensics & Security Laboratory, ***Asoto Technology Group***

11:00-12:00

Advanced Digital Forensic Process and tools for Law Enforcement and Intelligence Analysts

Alvaro Alexander Soto, Director of Digital Forensics & Security Laboratory, ***Asoto Technology Group***

1:00-2:00

The Basics of Weaponized Information

Stephen Arnold, Managing Partner, ***ArnoldIT.com***

Intelligence professionals have had a number of methods for injecting information into the media. These include social media, private newsfeeds, and the use of coordinated messages by contractors or other individuals. This session examines two case examples of using weaponized information to position an entity in public Web search results, within real time information streams, and in "conversations" in social media services. The upside, downside, and broad methodology of injection are reviewed in this one hour session. The formal remarks will be followed by a question and answer session.

2:15-3:15

Cell Phone Calls and Cell Tower Records for Investigators

Call Detail Records are the non-voice records generated by the use of a mobile phone. These records contain a wealth of potential evidence for analysts who know how to read and analyze them. In our session, we'll introduce attendees to CDR's, giving them practical skills they can use while working with these records.

Brent Bailey, ***Cellular Data Resources***

3:30-4:30

Cloud Lawful Interception and Data Retention

As cloud virtualization services and facilities scale rapidly worldwide, new sets of capabilities and needs are envisioned. Included in this ensemble are not only LI and data retention for cloud services and facilities, but also LI and data retention as diverse new cloud services. The designations LIaaS (LI as a Service) and RDaaS (Retained Data as a Service) encompass such implementations. The global law enforcement community and industry are working together on two new related work items dealing with these subjects in the ETSI TC LI standards body. Implementations are beginning to appear as offerings. This presentation provides an overview of the work and the related ISS industry opportunities.

Tony Rutkowski, VP, ***Yaana Technology***