TeleStrategies®

ISS World® South A

Intelligence Support Systems for Lawful Interception,
Elecronic Surveillance and Cyber Intelligence Gatherin

27 - 29 JULY 2015 • JOHANNE

ISS World South Africa is the world's largest gathering of Southern Africa 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: ISS for Lawful Interception and Criminal Investigations

Track 2: Encrypted Traffic Monitoring and IT Intrusion Product Training

Track 3: LEA and Intelligence Analyst Training and Product Demonstrations

Track 4: Social Network Monitoring and Big Data Analytics Product Demonstrations

Track 5: Mobile Location, Surveillance and Signal Intercept Product Demonstrations

Pre-Conference Seminars and Tutorials (Monday, 27 July 2015)

ISS World South Africa 2015 - Agenda at a Glance

Monday, 27 July 2015

Pre-Conference Training Seminars

Seminar #1
09:00-17:00

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***
09:00-10:00
The role of Online Social Media OSINT in Predicting and Interdicting Spree Killings: Case Studies and Analysis
10:15-11:15
OSINT and Criminal Investigations
11:30-12:30
Metadata Exploitation in Criminal Investigations
13:30-14:30
EXIF Tags and Geolocation of Devices for Investigations and Operational Security
14:45-15:45
Case Studies in Metadata Vulnerability Exploitation and Facial Recognition
16:00-17:00
What Investigators Need to Know about Emerging Technologies Used to Hide on the Internet

Seminar #2
08:30-16:30

Practitioners Guide to Internet Investigations

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

09:00-10:00

The World Wide Web and the Internet

10:15-11:15

Recognizing Traffic Data

11:30-12:30

WIFI and Mobile Data

13:30-14:30

Emerging Technologies, Masking Tech and Tools

14:45-15:45

Advanced Techniques in Tracing Suspects

16:00-17:00

Open Source Intelligence Training (OSINT)

Seminar #3
09:00-12:30

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.

09:00-10:00

Introduction to Telecom Infrastructure, Interception and Related ISS Products

10:15-11:15

Understanding Mobile Wireless Infrastructure, Interception and Related ISS Products

11:30-12:30

Understanding the Internet, Interception and Related ISS Products

Seminar #4
10:15-11:15

Bitcoin 101: Introduction to What Technical Investigators Need to Know about Bitcoin Transactions, Dark Web Commerce and Blockchain Analysis

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

This 101 training seminar is an introduction to Bitcoin, how the system is used to support criminal activities (e.g. Dark Web) and why technical investigators need to understand the basic Bitcoin transaction mechanism (Blockchain) to successfully defeat 21st century criminals and terrorist actions. Specifically this introduction to Bitcoin for technical investigators addresses:

- Bitcoin Basics for Technical Investigators
- Understanding Bitcoin Infrastructure, Blockchain and Bitcoin Mining
- How Criminals and Terrorists Use TOR and Dark Web
- Bitcoin Cryptography Demystified (For Non-Math Majors)
- Bitcoin 2.0 and the New Challenges Facing Law Enforcement

Seminar #5
11:30-12:30

Bitcoin 201: Setting Up a Live, Classroom Bitcoin Mining Platform in Order to Demonstrate Online, the Underlying Mechanisms of the Bitcoin System for Technical Investigators

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

Bitcoin 201 provides a hands-on demonstration of how to set up a Bitcoin mining platform in order to investigate Bitcoin Transactions and gather intelligence on criminal and terrorist activities via monitoring Bitcoin Blockchain archived and real-time ledger record flow. Specifically Technical Investigators will learn how to set up a Bitcoin Mining Platform.

- Bitcoin Core Client Software and where do you get it.

- Bitcoin Hardware and Software needed with cost consideration trade-off.
- Blockchain Analytics products available to gather intelligence from archived Bitcoin Ledger entries
- Keys and Bitcoin Addresses creation
- Bitcoin Investigator Platform Q&A

Seminar #6
13:30-14:30

Bitcoin 301: Classroom Demonstration of Submitting a Real Bitcoin Transaction to P2P Miners and viewing the recording in the Most Recent Blockchain and More Online Event Capturing Demonstrated

Presented by: *Matthew Lucas (Ph.D, Computer Science), Vice President,* ***TeleStrategies***
With a running Bitcoin Miner Platform as established in the previous session (Bitcoin 201), the operation will go live on the Bitcoin P2P network demmonstrating transaction precursory and intelligence gathering capabilities.
This session will demonstrate:

- How to establish a P2P Bitcoin network presence
- Generating a valid Bitcoin Transaction and following its acceptance in the Blockchain
- Note changes in resident Bitcoin Wallet after transaction placed
- Other Intelligence Gathering Capabiltities demonstrated along with Technical Investigation Q&A

VASTech Customer Workshop
10:00-16:00

10:00-12:00

Session 1: Mobile Monitoring Solution

Environmental scanning of an entire mobile network with geolocation and advanced analysis tools. Presentation and demonstration with real life use cases to effectively identify and capture suspects through information gathered strategically from a mobile network. Passive intelligence gathering, from land communications networks, plays a major role in identifying targets for the LI process. VASTech will discuss the Zebra system, with capturing and processing of millions of calls, to show how it can assist in identifying targets and benefit agencies in the intelligence communities

14:00-16:00

Session 2: Satellite Monitoring Solution

An introduction into a complete satellite monitoring solution spanning many different satellite technologies using case studies. Demonstration will be given on the most advanced satellite analysis software in the market.

A wealth of regional and transnational intelligence is available on satellite networks. Accessing satellite communications is not trivial due to the investment required in specialized skills and infrastructure. An operational database of satellite parameters is a strategic asset for national security.

Recent advances have significantly lowered the barriers to analyze and catalogue satellite carriers. It is now possible to get a clear picture of what information is out there, who it belongs to and whether it is of significance.

In this session we discuss the scope of the problem, a solution and accompanying benefits.

VASTech Customer Workshop requires a special registration. If interested go to www.vastech.co.za for registration information.

(Full Pre-Conference Seminar Agenda Appears After Track 5)

Tuesday, 28 July 2015

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 Com and Who at ISS World South Africa has Solutions**
*Dr. Jerry Lucas, President, **TeleStrategies***

ISS World South Africa Exhibits

28 July 2015, 10:00 a.m. - 17:00 p.m.

29 July 2015, 9:30 a.m. - 12:30 p.m.

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.

Monday, 27 July 2015

9:00-17:00 Session A	**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 Technolog Section,* ***Indiana State Police, USA***
9:00-12:30 Session B	**Understanding ISS Technologies and Products Deployed in Telecommunications Networ Monitoring Centers for Law Enforcement and Intelligence Analysts** *Dr. Jerry Lucas, President,* ***TeleStrategies***
13:30-17:00 Session B	**Understanding Bitcoin Infrastructure And Operations For Technical Investigators** *Matthew Lucas (Ph.D, Computer Science), Vice President,* ***TeleStrategies***

Tuesday, 28 July 2015

9:00-10:00 Session A	**Offensive Surveillance in Today's Changing, Challenging and Dangerous World and Soluti Law Enforcement** *Massimiliano Luppi, Key Account Manager,* ***Hacking Team***
9:00-9:30 Session B	**Home Invasion - Suspect discovery based on CDR data** *Presented by* ***trovicor***
11:30-12:00 Session A	**LI in Clouds, SDN & NFV"** This presentation discusses the consequences of cloud-based telecommunication services for LI. especially take a closer look at recent developments of SDN/NFV (software defined networking/network functions virtualization) and their relationship to clouds. *Presented by Rudolf Winschuh,* ***Utimaco TS GmbH***
11:30-12:00 Session B	**Scalable LI Solutions for dealing with LTE/VoLTE Roaming and OTT Encryption** *Michael Hammer, Principal Engineer,* ***Yaana Technologies***
12:00-12:30 Session A	**Enhancing mobile forensic investigations with data from the cloud** *Presented by* ***Cellebrite***
12:00-12:30 Session B	**Deep Packet Inspection in Clouds and NFV** *Curt Schwaderer, VP of Engineering,* ***Yaana Technologies***
14:00-14:30	**Big Data for Agency's & Telco's; Benefits in a Segmented & Shared Architecture** *Luis Alves, Senior Director Business Development,* ***AQSACOM***
14:30-15:00	**Demystifying SSL/TOR Interception: Attack case history and state-of-art Countermeasure** *Marco Valleri, CTO, Fabrizio Cornelli, QA Manager,* ***Hacking Team***

15:30-16:00 **Make Sure You Get All Data, and Get It Correct - even if it is hidden or been faked**
Presented by ***MicroSystemation***

Wednesday, 29 July 2015

9:00-9:30 **The Battle for Communication Security is Lost, or is it?**
Presented by ***Mils Electronic***

9:30-10:00 **Enterprise-Level Intercept Technology for the Edge User**
Presented by ***Ultra Electronics***

12:15-13:15 **Understanding Bitcoin along with TOR and Dark Web**
Matthew Lucas (Ph.D, Computer Science) and Vice President, ***TeleStrategies***

Track 2: Encrypted Traffic Monitoring and IT Intrusion Product Training

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

Monday, 27 July 2015

11:00-12:00 **FinFisher™: Maximum Impact - The Evolution of IT Investigation**
Presented by ***FinFisher***

Tuesday, 28 July 2015

9:00-10:00 **Covert IT Operations with OSINT and FinFisher™ - Real Scenarios**
Presented by ***FinFisher***

11:30-12:30 **Remote Exploitation of Smartphone and PCs - Reality vs Marketing**
Presented by ***FinFisher***

15:30-16:30 **Intruding personal devices with Remote Control System: Live Demo of latest attack and D Gathering Techniques**
Marco Valleri, CTO, Fabrizio Cornelli, QA Manager, ***Hacking Team***

Track 3: LEA and Intelligence Analyst Training and Product Demonstration Track

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

Monday, 27 July 2015

13:30-14:30 **CLOUD FORENSICS**
*Presented by **Cellebrite***

Tuesday, 28 July 2015

11:30-12:30 **Collecting, Processing, and Analyzing Multiple Communications Data Sources through On Pen-Link PLX**
*Presented by **Pen-Link***

14:00-15:00 **Second mobile phone discovery - An event based analytical approach**
*Presented by **trovicor***

15:30-16:30 **Cellebrite - UFED Series: Extract Insights. Focus Investigations - Unparalleled extraction a analysis optimized for lab and field**
*Presented by **Cellebrite***

Wednesday, 29 July 2015

9:00-10:00 **Speeding up criminal investigations - How to significantly decrease time necessary to ider targets**
*Presented by **trovicor***

11:00-12:00 **Who, What, When, Where - getting answers with help of right mobile forensic tools**
*Presented by **MicroSystemation***

Track 4: Social Network Monitoring and Big Data Analytics Product Demonstration Track

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

Monday, 27 July 2015

8:30-17:00 Session A **Practitioners Guide to Internet Investigations**
*Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement **Police***

9:45-10:15 Session B	**OSINT LABS from an empty building to a cornerstone of any Intelligence Organ** *Presented by* ***Gamma Group***
14:45-15:45	**Live Demonstration of SnapTrends: Real-Time Location-Based Social Intelligenc** *Presented by* ***Chenega International***

Tuesday, 28 July 2015

9:00-10:00 Session A	**Mobile Monitoring Solution: Find the needle in the haystack. Use cases for Law Enforce Agencies using location information and speaker identification.** *Presented by* ***VASTech***
9:00-10:00 Session B	**The New Investigator Toolbox: from Tactical to Open Source Investigations** *Presented by* ***AREA***
11:30-12:30 Session A	**Live Demonstration of SnapTrends: Real-Time Location-Based Social Intelligence** *Presented by* ***Chenega International***
11:30-12:00 Session B	**What OSINT can do especially when Multilingual and Multimedial** *Presented by* ***Gamma Group***
14:00-15:00 Session A	**SIGINT, OSINT, HUMINT: Massive Data Fusion, Search & Analytics in 3 clicks** *Presented by* ***Advanced Systems***
14:00-15:00 Session B	**Virtual Human Intelligence: be inside, stealth, future and technology proof. Some use ca** *Presented by* ***AREA***
14:00-14:30 Session C	**Intelligence in the Era of Global Terror - Boko Haram Case Study: Using Terrorists' O Communications in the Battle Against Them** *Guy Li-Ran,* ***Verint***
14:30-15:00 Session C	**Extend your reach and dominate your horizon - Beyond Borders: Gathering Intelligence Intelligence Operations in Rural and Semi-Urban Border Areas** *Moshe Samoha,* ***Verint***
15:30-16:30 Session A	**Big Data; Mass & Targeted Interception for National Security** *Julian Fellows, Executive Product Manager,* ***AQSACOM***
15:30-16:00 Session B	**How to Make Prisons into a Valuable Intelligence Source: Collect unparalleled informat your "agents" behind bars** *Moshe Samoha,* ***Verint***
16:00-16:30 Session B	**Catch Me If You Can: Identify an Offensive Youtube Video, Reveal the Poster, and Pinp Location** *Liad Churchill* ***Verint***

Wednesday, 29 July 2015

9:00-9:30 Session B	**From Intelligence to Action: Integrated and Versatile Intelligence Solutions for O Units** *Tomer Timor, **Verint***
9:30-10:00 Session B	**Fighting Targeted and Well-Funded Advanced Cyber Attacks** *Alon Wureit, **Verint***
11:00-12:00	**DPI and Social Media Analytics** *Curt Schwaderer, VP of Engineering, **Yaana Technologies***
12:15-13:15	**Top 20 Open Source Tools (OSINT) Used in Cybercrime Investigations** *Mark Bentely, Communications Data Expert, National Cyber Crime Law Enforcement **Police***

Track 5: Mobile Location, Surveillance and Signal Intercept Product Training

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

Monday, 27 July 2015

10:15-10:45	**GPS Tracking and the M2M for Surveillance operations** *Presented by **Gamma Group***

Tuesday, 28 July 2015

9:00-10:00 Session A	**High accuracy location intelligence for predicting and preventing crime** *Mahesh Patel, Chief Innovation Officer, **Polaris Wireless***
9:00-10:00 Session B	**Tactical Audio Monitoring via IP** *Presented by **Seartech***
11:30-12:30 Session A	**Satellite monitoring: All satellite data, one system. Play back of spectrum, analysis, int visualizing of data captured from a satellite.** *Presented by **VASTech***
12:00-12:30 Session B	**Utilizing readily available COTS devices to deliver a robust HUMINT collection capab** *Presented by **Gamma Group***
14:00-15:00	**Next-Generation Intelligence (Locate, Monitor targets Invisibly) with A.I Remote Con using Automation** *Manish Kumar & Rohitash Bhomia, **Wolf Intelligence***

Wednesday, 29 July 2015

11:00-12:00	**Nomadic equipment, wearable monitoring and field Command Centre** *Presented by* ***AREA***

Pre-Conference Training Seminars

Monday, 27 July 2015

Seminar #1
09:00-17:00

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***

9:00-10:00

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.

10:15-11:15

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.

11:30-12:30

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.

13:30-14:30

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.

14:45-15:45

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.

16:00-17:00

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 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 may become familiar.

Seminar #2
08:30-16:30

Practitioners Guide to Internet Investigations

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

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.

9:00-10:00

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

10:15-11:15

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.

11:30-12:30

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

13:30-14:30

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.

14:45-15:45

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

16:00-17:00

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

Seminar #3
9:00-12:30

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.

09:00-10:00

Introduction to Telecom Infrastructure, Interception and Related ISS Products

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.

10:15-11:15

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, MVNO'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, Instragram, Foursquare, VIBE and more).

11:30-12:30

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 #4
10:15-11:15

Bitcoin 101: Introduction to What Technical Investigators Need to Know about Bitcoin Transactions, Dark Web Commerce and Blockchain Analysis

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

This 101 training seminar is an introduction to Bitcoin, how the system is used to support criminal activities (e.g. Dark Web) and why technical investigators need to understand the basic Bitcoin transaction mechanism (Blockchain) to successfully defeat 21st century criminals and terrorist actions. Specifically this introduction to Bitcoin for technical investigators addresses:

- Bitcoin Basics for Technical Investigators: What's a bitcoin, basics of peer-to-peer electronic cash, who orchestrates the financial process, who champions Bitcoin commerce, how do consumers get started using Bitcoin and who handles the settlements

- Understanding Bitcoin Infrastructure, Blockchain and Bitcoin Mining: What's a Bitcoin Miner, what's needed to become one, why should law enforcement become Bitcoin miners, understanding Blockchain, transaction ledger records, how criminals do business anonymously using Bitcoins and how is all this orchestrated with no central authorities involved.

- How Criminals and Terrorists Use TOR and Dark Web: What's TOR, how does it function for basic anonymous communications, what's different with TOR Hidden Service (e.g. Dark Web), what is .ONION and how do criminals get started with setting up a Dark Web Merchandise site.

- Bitcoin Cryptography Demystified (For Non-Math Majors): The key to understanding why third party, financial institutions are not needed in Bitcoin transactions is understanding basic cryptography. This brief session explains how the system works starting with Bitcoin miners given an auto-generated "hash value" and challenged to add bits (nonce) to a block of Bitcoin transactions over the last 10 minutes along with how Bitcoin addresses (private and public encryption keys) are created. Webinar segment presentation time is less than five minutes for those not mathematically inclined.

- Bitcoin 2.0 and the New Challenges Facing Law Enforcement: Where is the Bitcoin phenomenon headed, what new application should investigators expect and the case for why Bitcoin will become the currency of Internet Commerce.

Seminar #5
11:30-12:30

Bitcoin 201: Setting Up a Live, Classroom Bitcoin Mining Platform in Order to Demonstrate Online, the Underlying Mechanisms of the Bitcoin System for Technical Investigators

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

Bitcoin 201 provides a hands-on demonstration of how to set up a Bitcoin mining platform to investigate Bitcoin Transactions and gather intelligence criminal and terrorist activities via monitoring Bitcoin Blockchain archived and real-time ledger record flow. Specifically Technical Investigators will learn how to set up a Bitcoin Mining Platform.

- Bitcoin Core Client Software: What hardware at a minimum is needed to monitor Bitcoin Blockchain not for profit (e.g. Winning New Bitcoin) but for intelligence gathering.
- Bitcoin Hardware and Software: Hash per second processing, electrical power requirements, Internet access speed requirements, blockchain storage, security considerations and more.
- Blockchain Analytics: Analysis tools available to search on Bitcoin Addresses. Big Data Analytics tools to connect the transaction slots and other basic program technical investigators should be aware of.
- Keys and Bitcoin Addresses: How to start the key generation process, from private (secret) key generator to public key and bitcoin Address generation. (Note, you don't have to be a math major to do this)
- Bitcoin Investigator Platform Q&A

Seminar #6
13:30-14:30

Bitcoin 301: Classroom Demonstration of Submitting a Real Bitcoin Transaction to P2P Miners and viewing the recording in the Most Recent Blockchain and More Online Event Capturing Demonstrated

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

With a running Bitcoin Miner Platform how to go live as a Peer-to-Peer Bitcoin Miner will be demonstrated. Again not to win new Bitcoins (virtually zero chance given the platform hash generation power) but to monitor live what's going on in the "Bitcoin Cloud".

- Establishing our Demonstration Platform Oerpator as a peer in the Bitcoin peer-to-peer network.
- Creating a Real, Valid Bitcoin transaction (Buyer to Seller), submitting it is the Bitcoin P2P network and watching it being made a part of the last 10 minute blockchain ledger.
- Submitting a non-valid Bitcoin transaction (e.g. erroneous private key signature) and monitoring the P2P rejection.
- Other Real Time bitcoin Network Monitoring Options for Technical Investigation.
- Technical Investigator Q&A

VASTech Customer Workshop
10:00-16:00

10:00-12:00

Session 1: Mobile Monitoring Solution

Environmental scanning of an entire mobile network with geolocation and advanced analysis tools. Presentation and demonstration with real life use cases to effectively identify and capture suspects through information gathered strategically from a mobile network. Passive intelligence gathering, from land communications networks, plays a major role in identifying targets for the LI process. VASTech will discuss the Zebra system, with capturing and processing of millions of calls, to show how it can assist in identifying targets and benefit agencies in the intelligence communities

14:00-16:00

Session 2: Satellite Monitoring Solution

An introduction into a complete satellite monitoring solution spanning many different satellite technologies using case studies. Demonstration will be given on the most advanced satellite analysis software in the market.

A wealth of regional and transnational intelligence is available on satellite networks. Accessing satellite communications is not trivial due to the investment required in specialized skills and infrastructure. An operational database of satellite parameters is a strategic asset for national security.

Recent advances have significantly lowered the barriers to analyze and catalogue satellite carriers. It is now possible to get a clear picture of what information is out there, who it belongs to and whether it is of significance.

In this session we discuss the scope of the problem, a solution and accompanying benefits.

VASTech Customer Workshop requires a special registration. If interested go to www.vastech.co.za for registration information.