

TeleStrategies®

ISS World America

Intelligence Support Systems for Lawful Interception,
Social Network and Dark Web Monitoring

11-13 SEPTEMBER 2017



WASHIN

-
-
-
-
-
-
-
-

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

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 networks, the Internet and Social Networks.

Track 1: ISS for Lawful Interception and Hi-Tech Criminal Investigations

Track 2: ISS for Real-Time Cyber Threat Detection

Track 3: ISS for Bitcoin Transaction and DarkNet Investigations

Track 4: Mobile Encryption Product Training for Secure Government Communications

Track 5: LEA, Defense and Interior Security Intercept Product Training

Track 6: Social Network Monitoring and Data Analytics Product Training

Track 7: Electronic Surveillance and Mobile Signal Intercept Product Training

Plus Advanced Hi-Tech, Cyber Crime Investigation Training Seminars (11 - 13 September 2017)

ISS World America 2017 - Agenda at a Glance

Training Seminars Led by Law Enforcement Officers and Ph.D Computer Scientists

28 classroom training hours, presented by sworn law enforcement officers, Ph.D. Computer Scientists and nationally recognized cybercrime textbook authors and instructors. Distinguished ISS World Training Instructors include:

Charles Cohen, Cohen Training and Consulting, LLC, also holds the position of Captain, Indiana State Police

(6 classroom hours)

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

(7 classroom hours)

Todd G. Shipley CFE, CFCE, President and CEO of Vere Software, Co-Author of , Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace and **retired Reno NV, Police Officer**

(6 classroom hours)

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

(4 classroom hours)

Jerry Lucas (Ph.D., Physics), President, **TeleStrategies**

(5 classroom hours)

Monday, September 11, 2017

Seminar #1

9:00-5:00 PM

Online Social Media and Internet Investigations

Presented by *Charles Cohen, Cohen Training and Consulting, LLC* Charles Cohen also holds the position of Captain, **Indiana State Police**

09:00-10:00 AM

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

10:15-11:15 AM

OSINT and Criminal Investigations

11:30-12:30 PM

Metadata Exploitation in Criminal Investigations

1:30-2:30 PM

EXIF Tags and Geolocation of Devices for Investigations and Operational Security

2:45-3:45 PM

Case Studies in Metadata Vulnerability Exploitation and Facial Recognition

4:00-5:00 PM

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

Seminar #2

9:00-5:00 PM

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. It is aimed primarily at the investigator, delivered from the perspective of detective, to empower them to have the best methodology and tradecraft to profile and catch suspects.

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

9:00-10:00 AM

The Internet, and how suspects leave a digital footprint

10:15-11:15 AM

Recognizing Traffic Data and digital profiling

11:30 AM-12:30 PM

WIFI, geolocation, and Mobile Data traces

1:30-2:30 PM

Awareness of Emerging Technologies, Masking Tech and Tools, TOR and proxies

2:45-3:45 PM

Advanced Techniques in Tracing Suspects and lateral problem solving

4:00-5:00 PM

Open source tools, resources and techniques

Seminar #3

9:00-5:00 PM

A Real World Look at Investigations in the Dark Web

Presented by: *Todd G. Shipley CFE, CFCE, President and CEO of Vere Software, Co-Author of , Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace and **retired Reno NV, Police Investigator***

The aim of this 1 day seminar is to take the attendees from the basics of understanding the Dark Web, how to access it to how to finding information hidden within it. The attendees will learn the best practices for the internet investigator when working in the Deep Web and the tools available to assist their investigations into the Deep Web.

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

09:00-10:00 AM

The Dark Web, what it is and what it is not

10:15-11:15 AM

To Tor or not to Tor

11:30 AM-12:30 PM

CryptoCurrency and its use in the Dark Web

1:30-2:30 PM

Going Undercover on the Dark Web

2:45-3:45 PM

Using web bugs and other technology to locate a suspect

4:00-5:00 PM

Advanced Dark Web Investigations, identifying the anonymous user

Seminar #4

9:00-12:30 PM

Understanding ISS Product Developments in Telecommunication Networks for Lawful Interception and Mass Surveillance

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

This half-day seminar covers what law enforcement and intelligence analysts need to understand about today's public telecommunications wireline and wireless networks as well as ISS technologies

and products used to lawfully intercept electronic communications and conduct mass network surveillance as discussed at ISS World Conference sessions and by exhibitors.

9:00-10:00 AM

Introduction to Wirelines and IP Infrastructure and Related ISS Products for Lawful Interception and Mass Surveillance

10:15-11:15 AM

Understanding Mobile Wireless Infrastructure, and Related ISS Products for Lawful Interception and Mass Surveillance

11:30 AM - 12:30 PM

Understanding the Internet Over-the-Top (OTT) Services and Related ISS Products for Mass Intelligence Gathering and Surveillance

Seminar #5

1:30-2:30 PM

Defeating Network Encryption: What Law Enforcement and The Intelligence Community Needs to Understand

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

The starting point to defeating encryption is to separate techniques addressing stored encrypted data such as with the Apple iPhone issue. The other challenge is defeating encrypted data in transit (e.g. Telegram, Whatsapp, etc.) or Network Encryption. This webinar is about defeating the later.

When it comes to defeating network encryption the technical community separates into two camps. Those who want to impede law enforcement and the government intelligence community from defeating network encryption: IETF, Silicon Valley and hundreds of third party encryption services. And your camp, those who want to investigate criminals and terrorist group who depend on network encryption.

Seminar #6

2:45-3:45 PM

Investigation Techniques for Unmasking TOR Hidden Services and Other Dark Web Operations

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

side that receives less attention are TOR hidden services. These are services that leverage TOR's anonymizing capabilities to mask the identity of criminally-hosted online services - forming the basis of just about all illegal gambling sites, drug markets, child exploitation material, firearm sales, terrorism propaganda, and more.

Tuesday, September 12, 2017

Seminar #7 **9:00-10:00 AM**

SS7 Network Vulnerabilities and Intercept Options

Presented by *Dr. Jerry Lucas, President, **TeleStrategies** and a Distinguished **Telecom Technology Expert** to be announced*

Last April's "60 Minute" episode on SS7 Network vulnerabilities sparked a lot of interest from privacy advocates, Congress as well as law enforcement and the government intelligence community. This session reviews the basics of SS7 Networks, how the "60 Minutes" team "legally" hacked into a call to Congressman Ted Lieu's office, how else someone could do the same without a large cooperative telecom and what else can be done with SS7 Networks access.

Seminar #8 **11:30 AM-12:30 PM**

The Implications of multi-IMSI and OTA for Law Enforcement and the Government Intelligence Community

Presented by *Dr. Jerry Lucas, President, **TeleStrategies** and a Distinguished **Telecom Technology Expert** to be announced*

The era of SIM Cards with static IMSIs issued by cellular operators is changing. Deployment of multi-IMSI as well as network programmable (OTA) SIM cards will create new challenges for law enforcement. This session looks at the implications of multi-SIM and OTA for LEAs and Intel analysts

Seminar #9

1:30-2:30 PM

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

Seminar #10

4:15-5:15 PM

Understanding Quantum Computers and How They Can Be Defeated with Quantum Safe Cryptography Options: QKD and PQC

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

This session first addresses why Quantum Computers when eventually deployed can defeat today's cryptosystems, a very briefly describes the Quantum Physics involved (e.g. Qubits, superposition and entanglements), the key crypto cracking computer algorithms (Shor and Grover) and the Quantum Computer performance metric to monitor.

The second part of this session will present the two defensive options: Quantum Key Distribution (QKD) via a Quantum Optic Channel and Post Quantum Cryptography (PQC) with no quantum physics, just newly developed cryptography algorithms.

Wednesday, September 13, 2017

Seminar #11
9:00-10:00 AM

The Computer Science View of Bitcoins

Presented by: *Nicholas Weaver, Ph.D. is a researcher at the International Computer Science Institute in **Berkeley**. His primary research is focused on network security, including worms, botnets, and other internet-scale attacks, network measurement, and network criminality including Bitcoin.*

The research community has devoted significant effort into understanding Bitcoin and the associated criminal activities < the results of which have promise to transform how law enforcement might handle Bitcoin investigations going forward. This speaker will present relevant Bitcoin/Dark Web investigation research including clustering to mass-deanonymize Bitcoin transactions, "tumblers" and Dark Markets; and why recording transactions is critical for de-anonymization success; robust estimates on the scale of Dark Markets and the daily volume of currency exchanged to/from Bitcoin (\$500,000/day); and experiments involving merging datasets with the Bitcoin blockchain < both of which reveal the MtGox accounts of multiple Silk Road drug dealers and was able to confirm that Sean Bridges (the Secret Service agent who stole from Silk Road) transferred effectively all his Bitcoins through MtGox.

Seminar #12
11:00 AM-12:00 PM

The Computer Science View of Dark Markets

Presented by: *Nicholas Weaver, Ph.D. is a researcher at the International Computer Science Institute in **Berkeley**. His primary research is focused on network security, including worms, botnets, and other internet-scale attacks, network measurement, and network criminality including Bitcoin.*

The research community has devoted significant effort into understanding Bitcoin and the associated criminal activities < the results of which have promise to transform how law enforcement might handle Bitcoin investigations going forward. This speaker will present relevant Bitcoin/Dark Web investigation research including clustering to mass-deanonymize Bitcoin transactions, "tumblers" and Dark Markets; and why recording transactions is critical for de-anonymization success; robust estimates on the scale of Dark Markets and the daily volume of currency exchanged to/from Bitcoin (\$500,000/day); and experiments involving merging datasets with the Bitcoin blockchain < both of which reveal the MtGox accounts of multiple Silk Road drug dealers and was able to confirm that Sean Bridges (the Secret Service agent who stole from Silk Road) transferred effectively all his Bitcoins through MtGox.

Pre-Conference Sessions Description At The End of Agenda Posting After Track 7

ISS World Americas 2017 Conference Agenda

September 13-15, 2016

ISS World America Exhibit Hours:

Tuesday, September 12, 2017: 10:00 AM-5:00 PM

Wednesday, September 13, 2017: 9:30 AM-12:30 PM

Tuesday, September 12, 2017

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

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

Track 1: ISS for Lawful Interception and Criminal Investigation

Tuesday, September 12, 2017

- 9:00-10:00 AM **SS7 Network Vulnerabilities and Intercept Options**
*Dr. Jerry Lucas, President, **TeleStrategies** and a Distinguished **Telecom Technology Expert** to announced*
- 11:30 AM-12:30 PM **The Implications of multi-IMSI and OTA for Law Enforcement and the Government Intel Community**
*Dr. Jerry Lucas, President, **TeleStrategies** and a Distinguished **Telecom Technology Expert** to announced*
- 1:30-2:30 PM **Lawful Intercept and Investigatory Insights from the Internet of Things (IoT)**
*Rick Robino, **Yaana Technologies (Invited)***
- 3:00-4:00 PM **100G Network Expansion and its Effect on Signals Intelligence and Intercept**
*Mike Seidler, Senior Product Manager, **NetQuest (Invited)***

Wednesday, September 13, 2017

- 9:00-9:30 AM
Session B **100GE Network Traffic Interception**
*Denis Matoušek, Product Manager, **Netcope (Invited)***
- 11:00 AM-12:00 PM
PM Session A **Metadata Correlation across CGNAT boundaries**
*Presented by **Napablaze (Invited)***

Track 2: ISS for Real-Time Cyber Threat Detection, Deep and Dark Web Monitoring

Monday, September 11, 2017

Tuesday, September 12, 2017

- 9:00-10:00 AM **Automated, Actionable, Affordable Dark Web Data Intelligence using Matchlight**
*Tyler Carbone, Chief Product Officer, **Terbium Labs (Invited)***
- 11:15 AM-12:15 PM
Session A **Putting the Wow into Intelligence**
*Darren MacLeod, Head of Product Marketing, **Verint, Communications & Cyber Intelligence Solutions (Invited)***
- 1:30-2:30 PM **OSINT Automation for Real Time Threat Detection**
*Justin Cleveland, Director of Federal Sales, **Recorded Future (Invited)***
- 3:00-4:00 PM **Diffeo Deep Web Discovery for Cyber Threat Analysis**
*John R. Frank, CEO and Co-Founder, **Diffeo (Invited)***
- 4:15-5:15 PM **Advanced Web Crawling and Scraping Technologies with a Dose of Artificial Intelligence and Machine Learning**
*Amanda Towler, PMP and Mark Hasse, Senior Software Engineer, **Hyperion Gray (Invited)***

Wednesday, September 13, 2017

9:00-10:00 AM
Session A

Disruptive Technology that Reduces Cyber Defense Complexity & Accelerates Investigation
Gary Woods, Director of Cyber Security Solutions NA, Verint, Communications & Cyber Intelligence Solutions (Invited)

Track 3: ISS for Investigating Criminal Bitcoin and DarkNet Transactions

Monday, September 11, 2017

9:00-5:00 PM

A Real World Look at Investigations in the Dark Web
Todd G. Shipley CFE, CFCE, President and CEO of Vere Software, Co-Author of Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace and retired Reno, NV, Police Officer (Invited)

Tuesday, September 12, 2017

1:30-
2:30 PM

Bitcoin 101: Introduction to What Technical Investigators Need to Know about Bitcoin Transactions and Dark Web Commerce and Blockchain Analysis
Matthew Lucas (Ph.D., Computer Science), Vice President, TeleStrategies

3:00-
4:00 PM

Bringing Transparency to Bitcoin transactions
This presentation will outline the cutting edge analysis techniques that Chainalysis employs to cluster Bitcoin addresses together and the different attribution strategies employed. Finally, using an example we will walk through a typical path an investigation may follow to get to a real world person.
Jonathan Levin, Co-Founder, Chainalysis (Invited)

4:15-
5:15 PM

Case Studies: Blockchain analysis in action
A case study focused presentation outlining the major threat actors and the anonymization techniques employed. Will step through some investigations outlining how to get leads in cases or look for corroborative evidence. Will step through some best practice when searching for Blockchain evidence, minimising the time wasted in investigation.
Jonathan Levin, Co-Founder, Chainalysis (Invited)

Wednesday, September 13, 2017

9:00-10:00 AM

The Computer Science View of Bitcoins
Nicholas Weaver, Ph.D. is a researcher at the International Computer Science Institute in Berkeley (Invited)

11:00 AM- 12:00
PM

The Computer Science View of TOR Hidden Services and Dark Markets
Nicholas Weaver, Ph.D. is a researcher at the International Computer Science Institute in Berkeley (Invited)

Track 4: Mobile Encryption Product Training for Secure Government Communications

Track sessions are for LEA and Other Government Attendees Only

Tuesday, September 12, 2017

4:15-5:15 PM

Understanding Quantum Computers and How They Can Be Defeated with Quantum Safe Cryptography Options: QKD and PQC
Dr. Jerry Lucas, President, TeleStrategies

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

Track sessions are for LEA and Other Government Attendees Only

Monday, September 11, 2017

9:00-5:00 PM

Practitioners Guide to Internet Investigations
Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement, UK Police

Tuesday, September 12, 2017

9:00-10:00 AM
Session B

Developing high capacity front ends for fiber and satellite mass signal capture systems
Presented by VASTech (Invited)

11:15 AM-12:15 PM
Session A

The New Forensic Investigator Toolbox: from Tactical to Open Source Investigation
Emanuele Marcozzi, Presales Engineer, AREA

11:15 AM-12:15 PM
Session B

Threat Actor Profiling: Gaining Targeted Intel on Cyber Criminals
Presented by Cybersixgill

1:30-2:30 PM Session
A

Correlating CDR with other data sources; succeeding against Anti-Forensics
Nicola Chemello, Chairman and Co-Founder, Securcube (Invited)

1:30-2:30 PM Session
B

Delivering a National Scale Data Intelligence Capability
Gordon Friend, Chief Engineer, BAE Systems Applied Intelligence

3:00-4:00 PM Session
A

IP Address Resolution - Breaking the Anonymity of Network Address Translation
Rick Robino, Yaana Technologies

4:15-5:15 PM Session
A

Post Trojan Infiltration: The new Digital Undercover Agent
Marco Braccioli, Senior Vice President and Emanuele Marcozzi, Presales Engineer, AREA

4:15-5:15 PM Session B **Advanced analytics to uncover targets and patterns based on mass data from a mobile phone and other communications capture systems**
Presented by VASTech (Invited)

Wednesday, September 13, 2017

9:00-10:00 AM **Forensic Data Fusion Centre: IPDR, CDR, Nat-Pat disambiguation and every external source in a single frame**
Marco Braccioli, Senior Vice President and Emanuele Marcozzi, Presales Engineer, AREA

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

Monday, September 11, 2017

9:00-5:00 PM **Online Social Media and Internet Investigations**
Charles Cohen, and Captain Indiana State Police, Cohen Training and Consulting, LLC

Tuesday, September 12, 2017

9:00-9:30 AM Session A **The Future of Crime Analysis: Empowering Law Enforcement Agencies with Artificial Intelligence**
Presented by Fifth Dimension (Invited)

9:30-10:00 AM Session A **"Minority Report" Comes to Life: The Science of Crime Prediction**
Presented by Fifth Dimension (Invited)

9:00-10:00 AM Session B **Social Media: How Adversaries do Reconnaissance and Deliver Payloads"**
James Foster, CEO, ZeroFOX (Invited)

11:15 AM-12:15 PM Session A **Finding Intelligence in Data with Network Visualization**
Presented by Cambridge Intelligence (Invited)

11:15 AM-12:15 PM Session B **Cyber Security: The Role of Government**
Gordon Friend, Chief Engineer, BAE Systems Applied Intelligence

3:00-3:30 PM Session A **Identify ISIS Recruiters Hidden in the Data with Artificial Intelligence**
Presented by Fifth Dimension (Invited)

3:30-4:00 PM Session A **Predictive Intelligence in Action: Reveal Terror Threats before they Become a Reality**
Presented by Fifth Dimension (Invited)

3:00-4:00 PM Session B **Web Intelligence - the next generation**
Alexander Aronovich, Senior Analyst, Verint, Communications & Cyber Intelligence (Invited)

4:15-5:15 PM **Advanced Analytics for Law Enforcement**
Prasanna Vijayan, Yaana Technologies (Invited)

Monday, September 11, 2017

Seminar #1
9:00-5:00 PM

Online Social Media and Internet Investigations

Presented by *Charles Cohen, Cohen Training and Consulting, LLC* Charles Cohen also holds the position of Captain, **Indiana State Police**

09:00-10:00 AM

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 AM

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 PM

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.

1:30-2:30 PM

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.

2:45-3:45 PM

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.

4:00-5:00 PM

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

9:00-5:00 PM

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. It is aimed primarily at the investigator, delivered from the perspective of detective, to empower them to have the best methodology and tradecraft to profile and catch suspects.

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

9:00-10:00 AM

The Internet, and how suspects leave a digital footprint

How it works. Why it works. How data traffic leaves a trace ; What the internet is; what is an IP and how is it significant to trace a person. IPv4 and IPv6 – understanding the changes- the benefits and pitfalls for the investigator. The internet has millions of copies of data on it - why, and where can we find this. Tracking and evaluating data

10:15-11:15 AM

Recognizing Traffic Data and digital profiling

What data is available. How to harvest and analyse it. Best practice to identify suspects and build profiles. Good practice, virtual data 'housekeeping' and tradecraft .Data collection and interrogation, significance and value. 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 analyse it. Investigator capabilities and opportunities.

11:30 AM-12:30 PM

WIFI, geolocation, and Mobile Data traces

A detectives 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. Unique communication identifiers . Dynamic live time tracing. Geo location services and uses. Online Surveillance and tracking movement and speed.

1:30-2:30 PM

Awareness of Emerging Technologies, Masking Tech and Tools, TOR and proxies

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. dynamic and pro active problem solving. Darknet, (Deep web) , TOR and IRC use. VOIP, Skype and FaceTime exploits. Advanced data sniffing and profile building. TOR systems, applications and ways to coax offenders out of the system.

2:45-3:45 PM

Advanced Techniques in Tracing Suspects and lateral problem solving

Using innovative and dynamic methods to trace offenders. Tricks used by suspects and how to combat them- Play them at their own game?. Covert internet investigations. Proxy servers and hiding. Managing collateral intrusion. Reverse and social engineering. Thinking outside the box. Lateral thinking. Possible missed opportunities. Profile building and manhunts through device footprints, speed and movement.

4:00-5:00 PM

Open source tools, resources and techniques

"Just google it" doesn't work anymore. A look at good tradecraft, practice and methodology in profiling, tracking and tracing digital footprints and shadows on the internet, by means of best available tools. A look at a selection of 200+ tools available on Mark's open source law enforcement tools website, that search engines cant see, with login and password provided during the session. Do's and do not's. Best tools for best results. When was the last time you 'googled' something in an investigation, and it returned 5 results, all specifically relating to your suspect? This session will teach you how.

Seminar #3

9:00-5:00 PM

A Real World Look at Investigations in the Dark Web

Presented by: *Todd G. Shipley CFE, CFCE, President and CEO of Vere Software, Co-Author of , Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace and **retired Reno NV, Police Investigator***

The aim of this 1 day seminar is to take the attendees from the basics of understanding the Dark Web, how to access it to how to finding information hidden within it. The attendees will learn the best practices for the internet investigator when working in the Deep Web and the tools available to assist their investigations into the Deep Web.

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

09:00-10:00 AM

The Dark Web, what it is and what it is not

In this block attendees will learn the background of what the really "Dark Web". The attendees will be able to identify the differences between the "Dark Web" and the "Deep Web"

10:15-11:15 AM

To Tor or not to Tor

This block will provide the attendees with an understanding of Tor, The Onion Router, and its use during law enforcement investigations. Also discussed will be management controls and investigative policy regarding its use in an undercover capacity.

11:30 AM-12:30 PM

CryptoCurrency and its use in the Dark Web

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

1:30-2:30 PM

Going Undercover on the Dark Web

In this block will be discussed the practical concerns and methods to be considered when going undercover on the "Dark Web". Also discussed will be the tools needed to be obtained for Internet investigations on the "Dark Web", agency policy concerns and how to document those investigations.

2:45-3:45 PM

Using web bugs and other technology to locate a suspect

Attendees will be exposed to techniques, using code and scripting inserted in various delivery methods, for revealing criminal Internet targets. The material covered will include tools available on the Internet and examples of scripting and techniques they can do themselves.

4:00-5:00 PM

Advanced Dark Web Investigations, identifying the anonymous user

This block will cover advanced concepts in the identification of targets over the Internet. Particularly focus will be on the available tools to law enforcement and the Intelligence community.

Seminar #4

9:00-12:30 PM

Understanding ISS Product Developments in Telecommunication Networks for Lawful Interception and Mass Surveillance

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

This half-day seminar covers what law enforcement and intelligence analysts need to understand about today's public telecommunications wireline and wireless networks as well as ISS technologies and products used to lawfully intercept electronic communications and conduct mass network surveillance as discussed at ISS World Conference sessions and by exhibitors.

9:00-10:00 AM

Introduction to Wirelines and IP Infrastructure and Related ISS Products for Lawful Interception and Mass Surveillance

- Wireline Interception Points
- PSTN Interception: Content, CDRs and MetaData
- Lawful Interception: Telecom to Monitoring Center
- Mass Metadata Surveillance and SS7
- IP Network Basics: Why IP Layers 1 to 7 needs to be understood
- Internet Access: Landline, Mobile, WiFi and others
- Deep Packet Inspection (DPI) and Intelligent Probes
- Optical Network Probe Intercept
- No. 1 Future Wireline Intercept Challenge: Network Function Virtualization

10:15 - 11:15 AM

Understanding Mobile Wireless Infrastructure, and Related ISS Products for Lawful Interception and Mass Surveillance

- Wireless Providers with Intercept Mandates and those with none
- Why Understand 2G, 3G, 4G and 4.5G Architecture need to be understood for Interception
- Wireless phone ID's and SIM cards
- Wireless Call Detail Record (CDR) Mining
- Wireless Data Services Option and Smartphone
- Cellular Roaming and Target Tracking with SS7
- Tracking and Location with IMSI Scanners and CDR Feeds

- Other Wireless Intercept: Satellite, Wi-Fi, WiMax and more
- No. 1 Future Wireless Intercept Challenge: True 4G and 4.5G
- ISS Products for Wireless Tracking Intercept and Mass Surveillance

11:30 AM - 12:30 PM

Understanding the Internet Over-the-Top (OTT) Services and Related ISS Products for Mass Intelligence Gathering and Surveillance

- What's meant by Over the Top (OTT)
- Understanding IP Layering for Lawful Interception
- Internet Players and NSP/ISP/IXP Intercept Infrastructure
- Social Network and Web Monitoring Techniques
- VoIP (Skype & VUPEN) Intercept
- TOR and Dark Web Intercept
- Bitcoin and Blockchain Traceback for LEAs and Intel
- No. 1 Future Internet Intercept Challenge: New IETF Privacy Standard Initiatives
- ISS Products for OTT Tactical and Mass Surveillance

Seminar #5

1:30-2:30 PM

Defeating Network Encryption: What Law Enforcement and The Intelligence Community Needs to Understand

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

The starting point to defeating encryption is to separate techniques addressing stored encrypted data such as with the Apple iPhone issue. The other challenge is defeating encrypted data in transit (e.g. Telegram, Whatsapp, etc.) or Network Encryption. This webinar is about defeating the later.

When it comes to defeating network encryption the technical community separates into two camps. Those who want to impede law enforcement and the government intelligence community from defeating network encryption: IETF, Silicon Valley and hundreds of third party encryption services. And your camp, those who want to investigate criminals and terrorist group who depend on network encryption.

Seminar #6
2:45-3:45 PM

Investigation Techniques for Unmasking TOR Hidden Services and Other Dark Web Operations

Presented by: *Matthew Lucas (Ph.D., Computer Science), Vice President, **TeleStrategies***
side that receives less attention are TOR hidden services. These are services that leverage TOR's anonymizing capabilities to mask the identity of criminally-hosted online services - forming the basis of just about all illegal gambling sites, drug markets, child exploitation material, firearm sales, terrorism propaganda, and more.

Tuesday, September 12, 2017

Seminar #7
9:00-10:00 AM

SS7 Network Vulnerabilities and Intercept Options

Presented by *Dr. Jerry Lucas, President, **TeleStrategies** and a Distinguished **Telecom Technology Expert** to be announced*

Last April's "60 Minute" episode on SS7 Network vulnerabilities sparked a lot of interest from privacy advocates, Congress as well as law enforcement and the government intelligence community. This session reviews the basics of SS7 Networks, how the "60 Minutes" team "legally" hacked into a call to Congressman Ted Lieu's office, how else someone could do the same without a large cooperative telecom and what else can be done with SS7 Networks access.

Seminar #8
11:30 AM-12:30 PM

The Implications of multi-IMSI and OTA for Law Enforcement and the Government Intelligence Community

Presented by *Dr. Jerry Lucas, President, **TeleStrategies** and a Distinguished **Telecom Technology Expert** to be announced*

The era of SIM Cards with static IMSIs issued by cellular operators is changing. Deployment of multi-IMSI as well as network programmable (OTA) SIM cards will create new challenges for law enforcement. This session looks at the implications of multi-SIM and OTA for LEAs and Intel analysts

Seminar #9
1:30-2:30 PM

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:

Seminar #10
4:15-5:15 PM

Understanding Quantum Computers and How They Can Be Defeated with Quantum Safe Cryptography Options: QKD and PQC

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

This session first addresses why Quantum Computers when eventually deployed can defeat today's cryptosystems, a very briefly describes the Quantum Physics involved (e.g. Qubits, superposition and entanglements), the key crypto cracking computer algorithms (Shor and Grover) and the Quantum Computer performance metric to monitor.

The second part of this session will present the two defensive options: Quantum Key Distribution (QKD) via a Quantum Optic Channel and Post Quantum Cryptography (PQC) with no quantum physics, just newly developed cryptography algorithms.

Wednesday, September 13, 2017

Seminar #11
9:00-10:00 AM

The Computer Science View of Bitcoins

Presented by: *Nicholas Weaver, Ph.D. is a researcher at the International Computer Science Institute in **Berkeley**. His primary research is focused on network security, including worms, botnets, and other internet-scale attacks, network measurement, and network criminality including Bitcoin.*

The research community has devoted significant effort into understanding Bitcoin and the associated criminal activities < the results of which have promise to transform how law enforcement might handle Bitcoin investigations going forward. This speaker will present relevant Bitcoin/Dark Web investigation research including clustering to mass-deanonymize Bitcoin transactions, "tumblers" and Dark Markets; and why recording transactions is critical for de-anonymization success; robust estimates on the scale of Dark Markets and the daily volume of currency exchanged to/from Bitcoin (\$500,000/day); and experiments involving merging datasets with the Bitcoin blockchain < both of which reveal the MtGox accounts of multiple Silk Road drug dealers and was able to confirm that Sean Bridges (the Secret Service agent who stole from Silk Road) transferred effectively all his Bitcoins through MtGox.

Seminar #12

11:00 AM-12:00 PM

The Computer Science View of Dark Markets

Presented by: *Nicholas Weaver, Ph.D. is a researcher at the International Computer Science Institute in **Berkeley**. His primary research is focused on network security, including worms, botnets, and other internet-scale attacks, network measurement, and network criminality including Bitcoin.*

The research community has devoted significant effort into understanding Bitcoin and the associated criminal activities < the results of which have promise to transform how law enforcement might handle Bitcoin investigations going forward. This speaker will present relevant Bitcoin/Dark Web investigation research including clustering to mass-deanonymize Bitcoin transactions, "tumblers" and Dark Markets; and why recording transactions is critical for de-anonymization success; robust estimates on the scale of Dark Markets and the daily volume of currency exchanged to/from Bitcoin (\$500,000/day); and experiments involving merging datasets with the Bitcoin blockchain < both of which reveal the MtGox accounts of multiple Silk Road drug dealers and was able to confirm that Sean Bridges (the Secret Service agent who stole from Silk Road) transferred effectively all his Bitcoins through MtGox.