ISS World Asia is the world's largest gathering of Regional Law Enforcement, Intelligence and Homeland Security Analysts, Telecoms as well as Financial Cyber Crime Investigators responsible for Cyber Defense, Electronic Surveillance and Intelligence Gathering.

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

Track 1: Lawful Interception and Criminal Investigation Training
Track 2: Defeating Encryption with IT Intrusion
Track 3: LEA, Defense and Intelligence Analyst Product Demonstrations
Track 4: Social Network/DarkNet Monitoring and Big Data Analytics Product Demonstrations
Track 5: Mobile Signal Intercept and Electronic Surveillance Product Demonstrations
Track 6: Investigating DarkNets and Associated Bitcoin Transactions
Track 7: Financial Crime: Prevention, Detection and Investigation

Training Seminars Led by Law Enforcement Officers and Ph.D Scientists (5 & 7 December 2017)

ISS World Agenda From 2017 ISS World Asia Program

ISS World Asia 2018
Agenda and Registration Link
Available September 2018

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

21 classroom training hours, presented by sworn law enforcement officers and Ph.D. Scientists

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***

(10 classroom hours)

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

(3 classroom hours)

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

(3 classroom hours)

Tuesday, 5 December 2017

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 Captain, Cyber Crimes Investigative Technologies Section, Indiana State Police, USA

09:00-10:00

Understanding Cell Handset Geolocation: What Investigators Need to Know

10:15-11:15

Open Source Intelligence (OSINT) Collection Tools: Creating an Inexpensive OSINT Toolbox

11:30-12:30

Metadata Exploitation in Criminal Investigations

13:30-14:30

Proxies, VPNs, Tor, Onion Routers, Deepnet, and Darknet: A Deep Dive for Criminal Investigators (Part 1)

14:45-15:45

Proxies, VPNs, Tor, Onion Routers, Deepnet, and Darknet: A Deep Dive for Criminal Investigators (Part 2)

16:00-17:00

Using Bitcoin and other Cryptocurrencies for Money Laundering and Contraband Procurement: Developing an Operational Understanding

Seminar #2
9:00-17:00

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.

09:00-10:00

The Internet, and how suspects leave a Digital Footprint

10:15-11:15

Recognizing Traffic Data and digital profiling

11:30-12:30

WIFI, geolocation, and Mobile Data traces

13:30-14:30

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

14:45-15:45

Advanced Techniques in Tracing Suspects, and lateral problem solving

16:00- 17:00

Open Source Tools, resources and techniques

Seminar #3
9:00-12:30

Understanding ISS Technologies and Products Deployed in Telecommunications Networks for Lawful Interception and Mass Surveillance

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

This half-day seminar covers how criminals and terrorists communicate over today's public telecommunications wireline and wireless networks, over the top Internet services and social networks. This seminar is ideal for law enforcement, interior security, public safety and others who need to understand the 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

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

10:15-11:15

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

11:30-12:30

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

Seminar # 4
13:30-14:30

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

Presented by: *Dr. 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 #5
14:45-15:45

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

Presented by: *Dr. Matthew Lucas, 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 #6
16:00-17:00

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

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

TOR networks are notoriously effective at hiding the online identity of criminals, terrorists and others who are up to no good. The other 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.

- How TOR hides IP addresses/identity/location
- TOR hosting, What is .ONION and content analysis

Thursday, 7 December 2017

Seminar #7
8:30-9:30

Practitioners Guide to Understanding Cyber Attacks on Banks - Exploring Vulnerabilities from The Perspective Of The Hacker

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

This one hour session will explore the viewpoints of both the banks perception of vulnerabilities, and that of the attacker. A follow-up session at 10:30 will address Practitioners Guide to Defending Banks Against Cyber Attacks.

Seminar #8
10:30-11:30

Practitioners Guide to Defending Banks Against Cyber Attacks – Identifying And Protecting Vulnerabilities To Frustrate The Thief, and Integrity Proof The Systems

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

This one hour session will explore the protection of weak points and future proofing banks agains cyber attacks.

Seminar #9
12:00-13:00

Top 20 Open Source Tools (OSINT) Used in Cybercrime Investigations

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

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

ISS World Asia 2017 - Conference Agenda

5-7 December 2017

Wednesday, 6 December 2017

Welcoming Remarks

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

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

ISS World Asia Exhibit Hours:

Wednesday, 6 December 2017

Hours: 10:00-18:00

Thursday, 7 December 2017

Hours: 9:30-12:30

Track 1: Lawful Interception and Criminal Investigation Training

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

Tuesday, 5 December 2017

13:30-14:30 **Next Generation of Monitoring Centre for Accelerated Investigation**
*Presented by **ClearTrail Technologies***

14:45-15:45 **Best Practices for Securing Government IT and Communications Infrastructure**

1. Common Cyber Security Threat Governments Must Deal with and New Types of At
States and Pirates (Ransomeware, etc.).
2. Common Security Weakness in Government IT and Communication Infrastructure.
3. Type of effective Cyber Security Communications Solutions Government should co

Moderator: *Jerry Lucas, President, **TeleStrategies***
Panel Presenter: *Mirko Minuzzo, **Feedback Italia***
Other ISS World Asia exhibiting Vendors to be invited.

Wednesday, 6 December 2017

9:00-9:30 **Lawful interception in 5G Mobile Networks**
This session will elaborate the needs and the challenges of lawful interception in cu
wireless networks. Network operators and law enforcement agencies will get practi

	about best practice techniques for the implementation of LI in 5G networks. *Presented by **Utimaco***
9:30-10:00	**Multi-source Intelligence Collection & Big Data Analysis** *Presented by **Sinovatio***
11:30-12:00	**Content Filtering – A Technical Answer to Data Growth** *Presented by **Utimaco***
12:00-12:30	**Speech Technologies applied to OSINT based Counter-Terrorism Analysis** *Presented by **Agnitio Now Part of Nuance***
14:00-14:30	**Lawful Interception Probe and Monitoring Center for LEA's** *Presented by **NORSI-TRANS***
14:30-15:00	**100% Signal Visibility within next generation communications networks** *Presented by **Lumacron Technology***

Thursday, 7 December 2017

8:30-9:30	**Update on Voice Data Mining for LEA, Military and Police** The presentation will provide update on the latest news in the field of Voice Biome Analytics for purposes of governmental sector. Attendees will gain knowledge abou trends from both technological and customer perspective. *Marek Slavik, **Phonexia***
10:30-11:00	**Man in the middle (Bridge, Reset, Close, SSL self signed, SSL CA signed, HTT** *Presented by **NORSI-TRANS***
11:00-11:30	**100GE Network Traffic Interception** *Presented by **Netcope Technologies***

Track 2: Defeating Encryption and IT Intrusion Product Training

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

Tuesday, 5 December 2017

10:15-11:15	**FinFisher™: Cyber Solutions for The Fight Against Crime** *Presented by **FinFisher***
13:30-14:30	**FinFisher™: Real-Life practical IT Intelligence Operations** *Presented by **FinFisher***
13:30-14:30	**Defeating Network Encryption: What Law Enforcement and The Intelligence C Understand** *Presented by: Dr. Matthew Lucas (Ph.D Computer Science), Vice President, **TeleStr***

Wednesday, 6 December 2017

14:00-15:00	**FinFisher™: Strategic and Tactical Wi-Fi Surveillance** *Presented by **FinFisher***

Track 3: LEA, Defense and Intelligence Analyst Training and Product Demonstrations

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

Tuesday, 5 December 2017

10:15-11:15	**Utilizing Technology in the Decision-Making Process** *Presented by **JSI Telecom***

Wednesday, 6 December 2017

9:00-10:00 Session A	**Lawful Interception in 2017. VoLTE and encrypted services like Facebook, Gmail and approach to the IP investigation** *Presented by **IPS***
9:00-10:00 Session B	**LIVE DEMO: face & voice recognition to identify people in video surveillance, phone media** *Presented by **ATIS***
11:30-12:30 Session A	**Latest updates on Forensic Investigator Toolbox** *Presented by **AREA***
11:30-12:00 Session B	**How to quickly and efficiently identify suspects** Live demonstration analysing complex data generated from multiple monitoring centers *Presented by **Trovicor***
12:00-12:30 Session B	**Real-time target location tracking** Live demonstration detailing how to generate intelligence from location information *Presented by **Trovicor***
14:00-15:00 Session A	**International Optic Fiber Analysis: Signals, Protocols, Metadata and Content all in on** *Presented by **VASTech***
14:00-15:00 Session B	**Generate Powerful Evidences from PCAP, CDR/IPDR and Social Media, all from a Si** Agencies have to deal with variety of data like PCAP, CDR/IPDR and Open Source Data et different sources. A typical investigation of such data involves manual correlation using different tools that ev disconnected intelligence and doesn't provide a single view of a "Person of Interest". What if you could bring data, tools and systems together on a single interface? Experience a seamless Investigation Workbench that assists investigators to collaboratively

	discover evidences, profile suspects, build stories and solve cases rapidly. *Presented by **ClearTrail Technologies***
15:30-16:30 Session A	**Big Data and Machine Learning for Intelligence: Cerebro NG** *Presented by **Advanced Systems***
15:30-16:30 Session B	**Hushmeeting: creating an iron-clad and quantum-safe communication environment** Preventing attacks, detecting intruders and collaborating within a backdoor-free and malwar communicaiton framework. Real use cases and attacking scenarios *Presented by **Feedback Italia***

Thursday, 7 December 2017

8:30-9:30 Session A	**Tracking Location and Calls of Foreign Nationals through the use of a Passive St Interception System** *Presented by **VASTech***
10:30-11:00 Session A	**Automatic Anomaly Detection: Recognizing pattern changes in targets' activities** *Presented by **Trovicor***
10:30-11:00 Session B	**Massive Investigation, with a care for privacy: Carrier Grade Nat disambiguatio Analysis** *Presented by **AREA***
12:00-13:00 Session A	**Top 20 Open Source Tools (OSINT) Used in Cybercrime Investigations** *Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcemen*
12:00-13:00 Session B	**Beyond Voice Biometrics. Upcoming Speech Analytics Technologies for Crimina** *Presented by **Agnitio Now Part of Nuance***

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

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

Tuesday, 5 December 2017

9:00-10:00	**How Public Sentiment can be influenced through propaganda campaigns on Soc** *Presented by **IPS***
11:30-12:00	**Extremist communication: what is out there, how to collect it, what it does, how and how to counter it – OSINT from a practitioners view** *Presented by **Gamma Group***
12:00-12:30	**Evidence-based, operational mission management – from the simple to the sophi** *Presented by **Gamma Group***

14:45-15:45	**Digital Investigations in dark net** *Presented by **AREA***

Wednesday, 6 December 2017

9:00-10:00	**AI Powered Web Intelligence** Extracting intelligent insights using machine learning algorithms *Presented by **CWA Webint Applications***
11:30-12:30	**Bridging discipline gaps in the hunt for perpetrators: Bringing together Metadata, OSI** **SIGINT, Dark Web, Surveillance techniques and various other capabilities to support l** *Presented by **Gamma Group***
14:00-15:00 Session A	**Dark Web – Can Governments afford not knowing? Hunting criminals on the dark sid** *Presented by **Gamma Group***
14:00-15:00 Session B	**GoldenSpear Deep WEBINT – Reaching the Deepest corners of the Deep Web and the** **DarkNet** *Presented by **S2T***
15:30-16:00 Session A	**Automatic Exploitation of Social Network, Deep and Dark Web to complement traditio** **Interception Infrastructure** *Presented by **IPS***
15:30-16:30 Session B	**Intelligence Analysis on Big Data** *Presented by **Sinovatio***
16:45-17:45 Session B	**Data Fusion and Analytics for National Security and Intelligence** *Presented by **Yaana Technologies***

Thursday, 7 December 2017

8:30-9:30	**Internet Records Intelligence: Collection, Storage, Disclosure and Analysis** *Presented by **Yaana Technologies***
12:00-13:00	**Ethical & Sustainable Solutions in the world of Encryption.** *Presented by **ClearTrail Technologies***

Track 5: Mobile Signal Intercept and Electronic Surveillance Training and Product Demonstration

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

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

Tuesday, 5 December 2017

11:30-12:30	**Command and Control Center for covert field operations using Audio, Video and** *Presented by **IPS***
13:30-14:30	**Satellite Monitoring Explained: Challenges and Solutions** *Presented by **VASTech***
14:45-15:45	**Innovative Image Recognition and Mobile Device Analytics to Create Actionable** Collecting and analyzing Automated Number Plate Recognition (ANPR), Facial Reco Device Data Capture and Ballistics Imaging to deliver real-time intelligence. These an and national security patterns, and unveil persons of interest and associations that may unnoticed. Vigilant Solutions' data fusion analytics enhance any agency's abilities to share information, which can be directly related to crime, terror threats, socioeconomi infrastructure, thereby increasing security and bolstering revenue generation. *Presented by **Vigilant Solutions***
16:00-17:00	**Cellular Intelligence in Action-Real use cases solved by combining mobile locatio from cellular networks** *Presented by **Mobilaris***

Wednesday, 6 December 2017

9:00-10:00 Session A	**RFID access control exploitation** *Presented by **Providence***
9:00-10:00 Session B	**Challenges in today's Inmarsat interception** Inmarsat enhances their services continuously. Thus the established and well-known intelli be adapted. What information is available and what can be done with it? *Ruediger Paetzold, **Rheinmetall Communication and Simulation Technology Pte. Ltd.***
11:30-12:30 Session A	**NeoSoft data traffic analyser for Mobile Monitoring** *Presented by **NeoSoft AG***
11:30-12:00 Session B	**GSM Tactical Interception System for 3G and 4G** *Presented by **Advanced Systems***
14:00-15:00 Session A	**Portable, Passive Monitoring tool for DPI and Multi-Dimensional Analysis** *Presented by **EXFO***
15:30-16:30 Session A	**Acquisition from Smart phone and WiFi-Data, incl. Geolocalization** *Presented by **Secure Information Management GmbH***
15:30-16:30 Session B	**Real-time, high accuracy mobile location tracking** *Presented by **Creativity Software***

Thursday, 7 December 2017

8:30-9:30	**IMSI Catcher, Target localization, Active and Passive Interception, Basics an** *Presented by **NeoSoft AG***

Track 6: Investigating DarkNets and Associated Bitcoin Transactions

This track is for law enforcement and private enterprise investigators who have to monitor and investigate the DarkNet along with Bitcoin transactions associated with criminal activities
Track 6 open to all government and commercial cyber crime investigators.

Tuesday, 5 December 2017

14:45-15:45

Bitcoin 101: Introduction to What Technical Investigators Need to Know abou Transactions, Dark Web Commerce and Blockchain Analysis
Presented by: *Dr. Matthew Lucas, Vice President, **TeleStrategies***

16:00-17:00

Investigation Techniques for Unmasking TOR Hidden Services and Other Da
Presented by: *Dr. Matthew Lucas, Vice President, **TeleStrategies***

Wednesday, 6 December 2017

9:00-10:00

Bitcoin in Practice
This is an introductory session to the practical uses of Bitcoin. By the end of this se comfortable with using and interpreting block explorers, methods of purchasing an the basic structure of Bitcoin transactions. This will include a demonstration of Ell analytics software.

- The blockchain - how to access and interpret it
- Using a block explorer
- How Bitcoin is used in practice: buying and selling, sending and receiving
- Bitcoin addresses and transactions

*Luke Wilson, Vice President of Business Development-Investigations, **Elliptic***
*Danielle Jukes, Investigator, **Elliptic***

11:30-12:30

Advanced Bitcoin Concepts and an Introduction to Bitcoin Investigations

Assuming an understanding of basic Bitcoin concepts, such as addresses and transactions, this session will cov such as mixing and address clustering. By the end of this session you should have an understanding of why the impact on tracing payments, and how they work in practice. We will also look at the basics of Bitcoin investig evidence, types of investigations, and contacting exchanges to identify Bitcoin users.

- Address clusters
- Mixers
- An introduction to Bitcoin analytics software
- Identifying Bitcoin evidence
- Types of Bitcoin investigations

· Identifying wallet holders

· Case study: ransomware

Luke Wilson, Vice President of Business Development-Investigations, ***Elliptic***
Danielle Jukes, Investigator, ***Elliptic***

14:00-17:45 **Special Half Day DarkNet Seminar**
by Andrew Lewman, Vice President, DarkOWL and Former Exectuve Direct

14:00-15:00

Indexing the dark net – how do you catalog and search something that is not meant to be easily scrubbe

Presented by:

Andrew Lewman, Vice President, ***DarkOWL***

15:30-16:30

Case studies / examples in dark net investigations – de-anonymizing examples / approaches / best practi

Presented by:

Andrew Lewman, Vice President, ***DarkOWL***

16:45-17:45
Future directions - what's next in dark net infrastructure, dark markets and i implications
Presented by:
Andrew Lewman, Vice President, ***DarkOWL***

Thursday, 7 December 2017

10:30-11:30 **Case Studies and Emerging Threats In the Criminal Use of Virtual Currencie**
(Only Open to Government and Law Enforcement Attendees)
The dark web economy is booming, thanks largely to the emergence of virtual curr quick, pseudonymous transfer of value across borders. In this session, we will expl studies showing how Bitcoin is being used to facilitate criminal activity and how b techniques have been used to counter this. We will also explore the new generatior such as Monero and Zcash, which promise much higher levels of anonymity, and v gaining traction on the dark web.
Luke Wilson, Vice President of Business Development-Investigations, ***Elliptic***
Danielle Jukes, Investigator, ***Elliptic***

Track 7: Financial Crime: Prevention, Detection and Investigation

This track is for law enforcement and private enterprise investigators who are responsible for money laundering, fraud prevention, detection and investigaiton and other cyber crime activities. Track 7 open to all government and private enterprise financial crime investigators.

Tuesday, 5 December 2017

4:00-5:00 **Using Bitcoin and other Cryptocurrencies for Money Laundering and Contraband Pro
Developing an Operational Understanding**

*Presented by: Charles Cohen, **Cohen Training and Consulting**, LLC Charles Cohen also
Captain, Cyber Crimes Investigative Technologies Section, **Indiana State Police, USA***

Wednesday, 6 December 2017

9:00-10:00
Session A

Protecting your organization from Insider Threats

The financial, reputational and regulatory impact of having an organization's critical assets stolen or damaged can be catastroph
access can exploit the vulnerabilities of critical assets, causing millions of dollars of damage. In order to reduce this risk, organi
program to protect their critical assets from an insider threat. These challenges lie in the fact that insiders are hidden in plain si
to detect.

Kanny Lee, an Executive Director from EY's Fraud Investigations team will be sharing practical insights and case studies on ho
effectively manage the risk of Insider threats by showcasing various forensic technologies and how it has applied to real life cas
We will cover topics such as:

- · Insights on best practices for using an Insider Threat Framework
  · Live demo on leveraging forensic data analytics for detection of high risk transactions
  · Applying digital forensics techniques to uncover what end users are actually doing (ch
  · Deployment of network forensics to discover malicious threats lurking in data traffic (
  hosts, etc)

  *Kanny Lee, Executive Director: Fraud Investigation & Dispute Services, **Ernst & Youn***

9:00-10:00
Session B

Bitcoin in Practice

This is an introductory session to the practical uses of Bitcoin. By the end of this session you sh
with using and interpreting block explorers, methods of purchasing and storing bitcoin, and the
Bitcoin transactions. This will include a demonstration of Elliptics' Bitcoin analytics software.

· The blockchain - how to access and interpret it

· Using a block explorer

· How Bitcoin is used in practice: buying and selling, sending and receiving

· Bitcoin addresses and transactions

*Luke Wilson, Vice President of Business Development-Investigations, **Elliptic***
*Danielle Jukes, Investigator, **Elliptic***

11:30-12:30
Session A

Leveraging Forensic Data Analytics to combat Financial Crimes

Technology can play a big role in helping to identify and detect crimes in motion. Leveraging big data technologies, organizatio
wide range of available data sources from internal and external channels to develop surveillance monitoring platform. By apply
organizations are able to make impactful use of aggregated datasets and objectively analyze suspicious behaviors that affect fin
Kanny Lee, an Executive Director from EY's Fraud Investigations team will be sharing practical insights on embedding your o
culture, preview of EY's Library of Risk Indicators and showcasing various dashboards used to aid in combating financial frau

- · Highlights from EY’s Forensic Data Analytics Survey
  · The essentials building blocks for a surveillance monitoring platform
  · Live demo on applying analytics to dissect cases such as: Retail Branch Theft, Swift E
  Banking
  · Tips on leading practices when deploying analytics for combating fraud
- *Kanny Lee, Executive Director: Fraud Investigation & Dispute Services,* ***Ernst & Youn***

11:30-12:30 **Advanced Bitcoin Concepts and an Introduction to Bitcoin Investigations**
Session B

Assuming an understanding of basic Bitcoin concepts, such as addresses and transactions, this session will cover more advance address clustering. By the end of this session you should have an understanding of why these concepts are useful, their impact o they work in practice. We will also look at the basics of Bitcoin investigations; how to identify evidence, types of investigations identify Bitcoin users.

· Address clusters

· Mixers

· An introduction to Bitcoin analytics software

· Identifying Bitcoin evidence

· Types of Bitcoin investigations

· Identifying wallet holders

· Case study: ransomware

Luke Wilson, Vice President of Business Development-Investigations, ***Elliptic***
Danielle Jukes, Investigator, ***Elliptic***

14:00-17:45 **Special Half Day DarkNet Seminar**
by Andrew Lewman, Vice President, DarkOWL and Former Exectuve Director, The TOR

14:00-15:00

Indexing the dark net – how do you catalog and search something that is not meant to be easily scrubbed? What’s possib

Presented by:

Andrew Lewman, Vice President, ***DarkOWL***

15:30-16:30

Case studies / examples in dark net investigations – de-anonymizing examples / approaches / best practices / lessons lear

Presented by:

Andrew Lewman, Vice President, ***DarkOWL***

16:45-17:45
Future directions - what’s next in dark net infrastructure, dark markets and investigation
Presented by:
Andrew Lewman, Vice President, ***DarkOWL***

Thursday, 7 December 2017

8:30-9:30 **Practitioners Guide to Understanding Cyber Attacks on Banks – Exploring Vulnerabiliti Perspective Of The Hacker**

This one hour session will explore the viewpoints of both the banks perception of vulnerabiliti

attacker. A follow-up session at 10:30 will address Practitioners Guide to Defending Banks Ag
Presented by: Mark Bentley, National Cyber Crime Law Enforcement, ***UK Police***

10:30-11:30 Session A **Practitioners Guide to Defending Banks Against Cyber Attacks – Identifying And Protect To Frustrate The Thief, and Integrity Proof The Systems**
This one hour session will explore the protection of weak points and future proofing banks agai
Mark Bentley, National Cyber Crime Law Enforcement, ***UK Police***

10:30-11:30 Session B **Case Studies and Emerging Threats In the Criminal Use of Virtual Currencies**
The dark web economy is booming, thanks largely to the emergence of virtual currencies that e
pseudonymous transfer of value across borders. In this session, we will explore a number of cas
how Bitcoin is being used to facilitate criminal activity and how blockchain analysis techniques
counter this. We will also explore the new generation of cryptocurrencies, such as Monero and
much higher levels of anonymity, and which are already gaining traction on the dark web.
Luke Wilson, Vice President of Business Development-Investigations, ***Elliptic***
Danielle Jukes, Investigator, ***Elliptic***

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

Tuesday, 5 December 2017

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 Captain, Cyber Crimes Investigative Technologies Section, Indiana State Police, USA

09:00-10:00

Understanding Cell Handset Geolocation: What Investigators Need to Know

10:15-11:15

Open Source Intelligence (OSINT) Collection Tools: Creating an Inexpensive OSINT Toolbox

11:30-12:30

Metadata Exploitation in Criminal Investigations

13:30-14:30

Proxies, VPNs, Tor, Onion Routers, Deepnet, and Darknet: A Deep Dive for Criminal Investigators (Part 1)

14:45-15:45

Proxies, VPNs, Tor, Onion Routers, Deepnet, and Darknet: A Deep Dive for Criminal Investigators (Part 2)

16:00-17:00

Using Bitcoin and other Cryptocurrencies for Money Laundering and Contraband Procurement: Developing an Operational Understanding

Seminar #2
9:00-17:00

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

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

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.

11:30-12:30

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.

13:30-14:30

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.

14:45-15:45

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.

16:00-17:00

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 nots. 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
9:00-12:30

Understanding ISS Technologies and Products Deployed in Telecommunications Networks for Lawful Interception and Mass Surveillance

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

This half-day seminar covers how criminals and terrorists communicate over today's public telecommunications wireline and wireless networks, over the top Internet services and social networks. This seminar is ideal for law enforcement, interior security, public safety and others who need to understand the 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

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

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

11:30-12:30

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
- Internt 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: Neew IETF Privacy Standard Initiatives
- ISS Products for OTT Tactical and Mass Surveillance

Seminar # 4
13:30-14:30

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

Presented by: *Dr. 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 #5
14:45-15:45

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

Presented by: *Dr. Matthew Lucas, 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 #6
16:00-17:00

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

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

TOR networks are notoriously effective at hiding the online identity of criminals, terrorists and others who are up to no good. The other 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.

- How TOR hides IP addresses/identity/location
- TOR hosting, What is .ONION and content analysis

Thursday, 7 December 2017

Seminar #7
8:30-9:30

Practitioners Guide to Understanding Cyber Attacks on Banks - Exploring Vulnerabilities from The Perspective Of The Hacker

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

This one hour session will explore the viewpoints of both the banks perception of vulnerabilities, and that of the attacker. A follow-up session at 10:30 will address Practitioners Guide to Defending Banks Against Cyber Attacks.

- What is the current typical attack

- Vulnerabilities leak points, and weak points

- Hacking the Bank by traditional social engineering

- Man in the middle/mobile (MITM)

- - Man in the Browser (MITB) attacks
- - DDOS, Zeus, Zbot, and other exploits
- - BHO poisoning (browser helper objects)
- - DNS poisoning
- - Pineapple and Rasberry Pi devices
- - Clickjacking
- - Formgrabbers
- - Cloning and contactless card vulnerabilities
- - PCI-DSS attacks and vulnerabilities
- - The hackers point of view

Seminar #8
10:30-11:30

Practitioners Guide to Defending Banks Against Cyber Attacks – Identifying And Protecting Vulnerabilities To Frustrate The Thief, and Integrity Proof The Systems
Presented by: *Mark Bentley, Communications Data Expert, National Cyber Crime Law Enforcement,* ***UK Police***

This one hour session will explore the protection of weak points and future proofing banks agains cyber attacks.

-PCI-DSS security and tightening

- -WiFi encryption to avoid MITM
- -Pen testing
- -Dynamic virus signatures and monitoring
- -End user verification and login
- -Customer vulnerabilities and verification
- -Quantum Dawn and Waking Shark II (wargaming) benefits
- -Future proofing and horizon scanning
- -Playing the hacker at his own game.

Seminar #9
12:00-13:00

Top 20 Open Source Tools (OSINT) Used in Cybercrime Investigations

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