"Hard-Core Computer-Aided Investigation, Open Source Intelligence (OSINT) and Digital Officer Safety"

April 5, 2019

Holiday Inn Chicago O'Hare Area
5615 N. Cumberland Avenue
Chicago, IL 60631

Seminar - Learning Objectives and Executive Summary:

Attendees will be introduced to critical sources and methods for gathering and using PII (Personally Identifiable Information), SPI (Sensitive Personal Information) and subjects' biographical data; will learn how to obtain and use Open Source Intelligence (OSINT); will receive hands-on instruction in cyber-investigative methods; and will receive instruction in digital counter-surveillance, including "Social Networking Best Practices" and "Digital Officer Safety".

This is an introductory (basic) course. No prior training or experience is necessary to attend this event. Upon completion of this course, attendees can expect to have achieved an understanding of how to use proprietary and Open Source data to support an investigative, auditing, compliance or security function and how to protect themselves, their organization and their activities and maintain OPSEC (Operations Security).

Persons successfully completing all seminar requirements will earn 8.0 CE hours. (Coding for CPEs: 5 CPEs will be earned in "Specialized Knowledge", 1 CPE in "Regulatory Ethics", and 2 CPEs in "Administrative Practice"). A Certificate of Completion will be provided.

This will be a live ("Group-Live"), hands-on seminar. Attendees are encouraged to bring active files and subject / target information for processing and/or to provide those files in advance.

This seminar is not open to the general public. Admission is at the sole discretion of the event coordinators and the presenters. Attendees will be required to show identification prior to entry to the event.

(c) 2019 Fraternal Order of Investigators

SCHEDULE:

0800-0900 - Registration (mandatory; includes identification verification)

0900-1200 - Module I

1200-1300 – LUNCH (Buffet Provided)

1300-1700 - Module II and Q&A

1730-1800 – Informal Networking Mixer (Bar Louis ; on Hotel premises)

Seminar Overview - General:

Numerous entities have put into practice operations that shred privacy and facilitate the gathering and warehousing of personal, relationship and communications data. Once unimaginable surveillance technologies are being perfected and implemented. The most intimate details of personal lives are routinely and unthinkingly self-contributed and surrendered to data-gatherers.

Self-contributed personal information gathered by private entities - Google, Facebook, Instagram, Snapchat, Twitter, Acxiom, et al - far exceeds information in governmental databases in both size and scope. Finances, sexual orientation, religion, politics, habits, hobbies, friends and family are gathered, indexed and analyzed.

Physical locations and activities are known, and past locations and activities are logged. If a subject attended a house of worship, or a demonstration, or visited an abortion clinic or a known criminal activity location or met with a targeted person, it was likely digitally documented.

Verified logins, cell phones and apps, Skyhook and known WiFi nodes, VOIP, Google Voice and Skype, facial recognition, camera analytics, license plate readers and advances in biometrics allow anyone to be de-anonymized and remotely observed.

Forensic linguistics, browser and machine fingerprinting and backdoors further eliminate the possibility of anonymous Internet activity.

Thanks to "The Internet of Things", your thermostat and electric meter report when you arrive home and your garbage can reports when you throw out evidence to be collected. Your baby's diaper tweets and your sexual activity is blogged by your wristband.

Data and "PII" (Personal Identifying Information) collection now begins at birth. No data gathered will ever be thrown away, and none of the data gathered belongs to you or is under your control. "Predictive profiling" knows what you will do and where you will go in the future, even if you don't.

Combining Open Source Intelligence (OSINT) with selected public records and proprietary databases allows a capable investigative or security professional to quickly, comprehensively and covertly compile a comprehensive dossier on any subject, witness or target.

(c) 2016 - Fraternal Order of Investigators

ADDITIONAL SEMINAR COMPONENTS :

This seminar will discuss and demonstrate methods of merging proprietary online databases with public records, OSINT (Open Source Intelligence) and free sources, to support "skip trace", background, character, due diligence, criminal, civil and asset-location investigations, and will include a review of proper case intake, to facilitate effective OSINT activity. **Attendees are encouraged to submit active files for processing at least one (1) week before the event**.

This seminar will also include an "ethical investigating" component (1.0 hour/CE), including discussion of laws governing data access (ex. FCRA, DPPA, GLB) and use of OSINT methods (e.g. adherence to bar association no-contact rules, restraining orders, etc.).

This seminar, time permitting, will also include introductory instruction in tracing e-mail addresses, domain names (URLs) and IP addresses to owners / users and physical locations.

This is an introductory level course. No prior training or experience is necessary.

"Digital Officer Safety":

This seminar will include "Digital Officer Safety" and "Social Networking Best Practices" components. The purpose of these counter-intelligence (CI) segments is to provide awareness and digital self-defense training to investigative and other professionals who might be targeted online by criminals.

"Digital Officer Safety" is a critical concern, as radicals and criminals routinely use the Internet, Open Source Intelligence (OSINT) and public records to target law enforcement and other investigative professionals. “Doxing”, “Dorking”, “crowd-sourced investigation”, facial recognition, public “people finder” databases, “Google-Fu” and other open source tools and methods are used by persons with criminal intent to obtain investigative and law enforcement professionals’ home addresses, spouses’ and children’s names, photos, license plates and countless other types of sensitive information. Today, any interested person with bad intent can build a dossier on a target in a matter of minutes. Information gathered online by criminals and radicals can be later used to impede and terrorize, and even to facilitate direct or indirect physical attacks (ex. “SWAT-ing”) on Investigators and law enforcement at their work, in the field and in their homes.

Eric Garner’s wife tweeted the home addresses of NYPD officers involved in her husband’s arrest. Occupy Wall Street used facial recognition technology and crowdsourcing to identify arresting officers and their family members. Daesh and other terrorist groups routinely post personal information of deployed members of the military with a suggestion that they be attacked.

The "Digital Officer Safety" and "Social Networking Best Practices" components of this seminar will provide attendees with basic awareness and tools necessary to mitigate digital threats.

(c) 2017 Fraternal Order of Investigators

COST – POLICIES

COST: $ 159.00

Application and payment must be received from all prospective attendees prior to the event.

All payments by check must be drawn on a U.S. bank. Payment by credit card accepted. Please use the attached form. Online payment may be made via ADSAI's online payment link at: http://www.adsai.org/ .

DISCOUNTS – This Event Only:

$25.00 discount for FOI, ADSAI, NADDI, ISPA, ILASPPS members in good standing, independent Law Enforcement Oficers and for members of all other co-sponsoring / cooperating associations.

Refund Policy – This Event Only:

40% refund for cancellation until 25 March 2019.

NO refund for cancellation after 25 March 2019.

Substitution of attendee permitted until 30 March 2019.

Suggested Attire:

Business Casual recommended.

Payment:

Registration and payment can be made by use of the attached forms. All payments by check should be payable to "Fraternal Order of Investigators" and drawn on a U.S. bank.

Venue Comments:

"Located 2 miles from O'Hare International Airport, fully renovated as of April 2018, free parking, hotel rooms available at low discount rate with no offer code needed."

CEs / CPEs and Copies of Slides:

To obtain Continuing (Professional) Education credit hours and/or copies of event slides a Speaker Evaluation Form must be completed and submitted on-site. No exceptions possible. CEs are granted at no extra cost and are accepted nationwide.

(c) 2016 Fraternal Order of Investigators

STEVEN RAMBAM

CFE, CPP, PSP, PCI, CSAR, CFCS, BCIP (Cand.)

PRINCIPAL INSTRUCTOR

Steven Rambam is the founder and CEO of Pallorium, Inc., a licensed Investigative agency and security services provider. Since 1981, Pallorium's investigators have successfully closed more than 10,000 cases worldwide, ranging from homicide and death claim investigations to missing person cases to the investigation of various types of sophisticated financial and insurance frauds.

Steven is also the host of a reality network television show and a weekly radio show.

Steven Rambam has lectured on topics ranging from "the location of missing persons", to "the criminal use of false identification", to "foreign investigations", to "war crimes and the pursuit of war criminals". Steven's keynote lectures, "Privacy Is Dead - Get Over It" and "International Investigations", have received worldwide recognition including a "Speaker of the Year" award.

Steven is a recognized SME on the topics of “Computer-Aided Investigation”, “Open Source Intelligence (OSINT)” and “Digital Officer Safety” and he provides regular instruction on these topics to private and governmental agencies.

Steven holds the "CFE" board certification from the Association of Certified Fraud Examiner, the "CPP", "PSP" and "PCI" board certifications from ASIS International, the "CSAR" certification from the International Association of Asset Recovery Specialists and the "CFCS" certification from the Association of Certified Financial Crime Specialists.

Steven is a member of FOI (Founding Member), WAD (Life Member), NAIS (Life Member), ION, AIIP, NCISS (National Board Member), BOMP (Founding Member), COIN, IJI, IOA, TALI, FALI, ACFE, ASIS, ACFCS, IWWA, ALDONYS (Board Member and Regional Director), SPI (former VP and Board Member) and other investigative, law enforcement and security associations.

For more information and contact details: www.pallorium.com and www.stevenrambam.com.

(C) 2015 - International Order of Investigators

FRATERNAL ORDER of INVESTIGATORS
www.fraternalinvestigators.org
P. O. Box 155, Brooklyn, NY 11230

"Hard Core Computer-Aided Investigation, Open Source Intelligence and Digital Officer Safety"

Chicago, Illinois
05 April 2019

(Amount Paid: $_____)

PLEASE RETURN THIS SHEET WITH PAYMENT

YOUR NAME: _____
(Please Print Name)

CURRENT FOI MEMBER (CIRCLE ONE)? YES / NO

AGENCY or COMPANY : _____

ADDRESS: _____

OFFICE TELEPHONE: _____ CELLULAR: _____

E-MAIL: _____

ASSOCIATION AFFILIATIONS (other than FOI): _____

I REQUEST BCIP / CONTINUING EDUCATION (CE) CREDITS : ( ) YES ( ) NO

THIS EVENT IS NOT OPEN TO THE GENERAL PUBLIC.

http://www.fraternalinvestigators.org

(c) 2016 - Fraternal Order of Investigators

CREDIT CARD CHARGE AUTHORIZATION

I,_____ ,
(enter YOUR COMPLETE NAME as it appears on your credit card)

residing at / doing business at:_____,
(enter the COMPLETE BILLING ADDRESS and ZIP CODE for your card)

with a daytime telephone number of: _____,
(enter your DAYTIME TELEPHONE NUMBER here)

authorize Pallorium, Inc., to charge my credit card:_____,
(enter your CREDIT CARD NUMBER here)

expiration date: _____/20_____, Security Code: _____, the amount of: $_____,
(print or type your card's expiration date and security / PIN code)

as payment for admission to: **"OSINT – Chicago, IL – April 5, 2019"** by the following persons:

1. _____
2. _____
3. _____
4. _____
5. _____

I have read and agree to all policies established for this event.

_____, _____/_____/20_____ .
(Cardholder signature here) (today's date here)

Once completed, please return this sheet by fax or email (rambam@pallorium.com).

American Express, Mastercard or Visa are accepted for this event.

• P. O. BOX 155 • MIDWOOD STATION • BROOKLYN • NEW YORK 11230 USA •
• TELEPHONE: (001) 212-969-0286 • FAX (001) 212-858-5720 •

(c) 2016 - Fraternal Order of Investigators

POLICIES – ALL EVENTS - Fraternal Order of Investigators

Refunds:

A full refund is offered whenever a class is cancelled or rescheduled.

Please see this event's Policies and Notes for event-specific refund policies.

Program Cancellation:

Effort will always be made to preserve stated course content, scheduling and location. In the event that it proves impossible to provide the offered course in the offered location, a decision will be made as soon as possible to reschedule or move to an alternate location, and all registered attendees will be notified immediately. In the event of cancellation of any course or event, all registered attendees will be notified immediately by electronic mail. All registered attendees must provide FOI with a current e-mail address and telephone number.

We strongly recommend that all attendees subscribe to FOI's Twitter feed (@FOInvestigators) to allow for backup notification.

Programs will only be permanently cancelled in the event of permanent unavailability of an irreplaceable instructor.

Complaint Resolution:

All complaints are handled by FOI's Education Chairman or the President of the Advisory Board on a case-by-case basis.

Complaints regarding course content, accuracy of course description or an instructor's competence or conduct will be resolved within ten (10) business days and, if found to be valid, will result in a full refund to the complainant of all fees paid.

The Fraternal Order of Investigators is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.learningmarket.org.

[Note: all FOI courses are periodically modified and updated to remain current with evolving best practices, law, and technologies.]

(c) 2016 - Fraternal Order of Investigators

FOR QUESTIONS AND ASSISTANCE, PLEASE CONTACT THE FOLLOWING EVENT COORDINATORS:

Steven Rambam,
CFE, CPP, PSP, PCI, CSAR, CFCS, BCIP (Cand.)
TEL. 212-969-0286
edchair@fraternalinvestigators.org
rambam@pallorium.com

Kathryn LeFevour, PCI
A.D.S.A.I. Secretary
312-666-5114
info@lefevourpi.com

Bia Tyk
A.D.S.A.I. President
(630) 655-1313
bia@tricoinvestigations.com

"Informal Networking Mixer"

There will be an **Informal Networking Mixer** following the seminar.

1730-2000

Bar Louie O'Hare
(located on-site in the Holiday Inn Chicago O'Hare Area Hotel)

CASH BAR and BYOF (Buy Your Own Food)

All attendees, their guests and members of ADSAI, FOI and other professional associations are welcome.

(c) 2016 - Fraternal Order of Investigators