PATC NEWS

Follow PATC by Mail, Email or Online

PRESORTED
STANDARD
POSTAGE & FEES
PAID
INDIANAPOLIS, IN
PERMIT NO. 1547

E-NEWSLETTER

FREE LEGAL UPDATES & TRAINING ANNOUNCEMENTS BY EMAIL

TRAINING BROCHURES

TRAINING BROCHURES BY POSTAL MAIL

LEGAL UPDATES & TRAINING ANNOUNCEMENTS ON

Find us on Facebook

PATC - PUBLIC AGENCY TRAINING COUNCIL

@PATC updates

twitter

Instagram

@PATC updates

Please visit our website at www.patc.com for a full detailed schedule and description of each course.

Public Agency Training Council
2230 Stafford Road
STE 115
Plainfield, IN 46168

Phone: 1-800-365-0119
Fax: 317-821-5096
Email: questions@patc.com

Visit us on the Web at:
www.patc.com

Public Agency Training Council

Mark Waterfill, President

National Criminal Justice
Public Safety Continuing Education

Sponsored By:
Columbus Police Department
Columbus, Ohio

Training Seminar
Social Media and OSINT Investigative Techniques

Instructor:
Melissa Maranville

Melissa is the Founder/CEO of DeVille and Associates, LLC, located in Knoxville, Tennessee, USA. DeVille offers Forensic Consulting and Training to law enforcement and other criminal justice professionals. DeVille consults, develops content, and trains on complex topics such as cryptocurrency, surface/dark webs, bots, AI, social media, cybercrime, predator behavior, OSINT, and linkage analysis. Melissa has partnered with many linkage analysis and OSINT companies offering trainees insight and access.

Melissa began her criminal justice career as a booking and intake officer at Knox County Sheriff's Department in Knoxville, TN, and a student of Dr. Bass of the "Body Farm," Forensic Anthropological Research Facility, and since has dedicated her career to researching and developing content for criminal justice education and training for over 30 years. In addition, she provides education and training to social media and gaming moderators investigating cyber predators, CSAM, and violent content for blue chip companies. Lastly, Melissa is also a forensic consultant for human trafficking divisions within law firms.

Melissa's education includes bachelor's and master's degrees from the University of Tennessee in Knoxville, TN, and a Ph.D. (candidate) from Grand Canyon University in Phoenix, Arizona. Her dissertation topic is "A Case Study of Ineffective Legislation: Moral Panic and the Sex Offender Registry." When she concludes her Ph.D., she hopes to influence new sex offender legislation in tracking and tracing registered and non-registered sex offenders.

November 6 & 7, 2024
Columbus, Ohio

Social Media and OSINT Investigative Techniques

Course Description

The criminal mind never sleeps and is constantly advancing with technology. This introductory course will review the use of cyber technology, discussing web platforms, AI and bot technology, linkage analysis, and social networking sites such as Facebook, Instagram, Tumblr, Twitter, Google+, Telegram, Omegle, Discord, Twitch, Spotify, and many others to understand cybercrime. Social networking sites and cell phones have expanded cybercrimes and created new channels for sharing information that could also be utilized by law enforcement to investigate crimes and identify suspects. With using OSINT, there are many techniques that can be used to gather intelligence across the internet and social media platforms. Examples of OSINT include tracing usernames, emails, text hide software, phone number searches, OSINT dashboards, reverse images, websites, screen catch, trace and track linkage analysis, and so much more.

This course includes many OSINT tools and how to create a sock puppet for cyber investigations. This course primarily focuses on Open-source Intelligence (OSINT) and social media, chat, and gaming platforms; however, those are also available on cell phones. We will touch on OSINT that can be used for cell phones and we will review networking, routers and how to conduct a router interrogation, step-by-step. This course also includes information on warrant templates for over 500 social media and gaming platforms discussing some of the most common and what each one collects regarding IP addresses, URLs, voice, pictures, videos, financial data, and much more. We will also be discussing current case studies using linkage analysis, OSINT, and technological combinations used for success. We will close the training by discussing the importance of 3-D digital evidence and courtroom testimony. Most case studies include sextortion and other sex crimes as examples.

*Course will not be taught in necessarily the same order as listed below and in outline. Bring tools for taking notes. Computer not required but encouraged. (2-day event)

Upon Completion Participants will be able to:

1. Common crimes committed on social networking sites.
   - The use of “bots.”
   - Artificial intelligence in gathering data.

2. Understand the basic steps for preserving a profile.
   - Identifying its creator.
   - Set up undercover profiles (steps in creating a sock puppet)
   - Gather profile information.
   - Importance of email addresses and usernames in linkage analysis.

3. . Review social networking sites
   - Obtain evidence from servers and OSINT.

4. How to create and use a sock puppet for undercover investigations.
5. Review step-by-step router interrogations
   - Analyze routers at the scene.

6. Digital evidence and courtroom testimony.
7. Understand and define the basic terms related to investigating cybercrimes.
8. Understand and explain cyber data.
   - Including Dark Web ad virtual private networks (VPNs)
   - Capture IP addresses, URLs, Metadata, and more

9. Describe the links between social networking sites and the acceleration of crimes.
   - Telegram, Omegle, Chat investigations, gaming platforms and more platforms.

10. Understand the role of sextortion and online gaming platforms using social networking sites and cell phones.
11. Employ specific techniques and evolving tactics for successful cyber investigations.
12. Learn how to intercept digital evidence.
    - Learn the importance of securing metadata when intercepting evidence.

Sites that do not collect metadata and why.

Seminar Agenda
Social Media and OSINT Investigative Techniques
November 6 & 7, 2024

November 6, 2024	
8:30am – 9:00am	Registration
9:00am – 9:30am	Introduction: Why the Internet? What are the questions needing to be answered? Challenges
9:30am- 10:30am	Understand and define the basic terms related to investigating cybercrimes. Common crimes committed on social networking sites. The use of “bots” in collecting data Artificial intelligence in gathering data. a. Web 1, 2, & 3
10:30am – 11:00am	Understand and explain servers. Including dark web and virtual private networks (VPNs)
11:00am – 12:00pm	Surface and Dark Web
12:00pm – 1:00pm	Lunch
1:00pm – 2:00pm	Describe the links between social networking sites and the acceleration of crimes. Telegram, Omegle, Google, FB, IG, WhatsApp, Kik, and so much more. What data is specifically collected by each social media platform? Access to over 500 social media and gaming platforms’ data.
2:00pm – 2:30pm	Case Studies Understand the role of sextortion and other crimes using online gaming platforms and social networking sites.
2:30pm –3:30pm	OSINT Dashboards and Linkage Analysis
3:30pm – 4:30pm	Capture digital evidence from computers and net works using OSINT. Employ specific techniques and evolving tactics for successful cyber investigations. Importance of using OSINT combinations
4:30pm – 5:00pm	Q & A
November 7, 2024	
8:30am – 9:00am	Good morning, and Welcome! Brief review from the prior day and Q&A
8:30am – 9:00am	Search warrant templates Prepare a search warrant for data stored on different \ platforms. OSINT for search warrant templates and paid for software. Warrant templates for most social media sites. Profile information, emails, usernames Voice, photo and video data, financial information, and more IP addresses, URLs, Metadata, and more How to analyze routers at the scene The dos and don’ts
9:00am – 11:00am	Understand the basic steps for preserving public social media profiles and warrants.
11:00am – 12:00pm	Steps to developing a sock puppet for undercover investigations.
12:00pm. – 1:00pm	Lunch
1:00pm. – 2:00pm	Sock puppet continued and OSINT.
2:00pm – 3:00pm	Review step-by-step router interrogation.
3:00pm – 4:30pm	Court Room Testimony Presenting digital and electronic evidence. Issue with Jurors
4:30pm – 5:00pm	The Future and Q & A What Can We Do?

3 Ways to Register for a Seminar!

1. ***Register Online*** at **www.patc.com** — Yellow link upper left corner
2. ***Fax Form*** to Public Agency Training Council **FAX: 1-317-821-5096**
3. ***Mail Form*** to

Public Agency Training Council
2230 Stafford Road
STE 115, PMB 379
Plainfield, IN 46168

Federal ID# 47-4078912

*** **Pre-payment is not required to register** ***

Upon receiving your registration we will send an invoice to the department or agency .

Checks, Claim Forms, Purchase Orders should be made payable to:
Public Agency Training Council

If you have any questions please call
317-821-5085 (Indianapolis)
800-365-0119 (Outside Indianapolis)

Seminar ID SMOIT-002

Seminar Title: **Social Media and OSINT Investigative Techniques**

Instructor: **Melissa Maranville**

Seminar Location: **Columbus Ohio Division of Police Training Academy**
1000 North Hague Avenue
Columbus, OH 43204

When: **November 6 & 7, 2024**

Registration Time: 8:00 A.M. (June 18, 2024)

Hotel Reservations: **Drury Inn & Suites Columbus Convention Center**
88 E. Nationwide Blvd.
Columbus, OH 46215
Phone: 614-221-7008
Contact Hotel for Current Rates (plus tax)

Registration Fee: $350.00 Includes Social Media and OSINT Investigative Techniques Course Material and Certificate of Completion.

Names of Attendees 1. _____

2. _____

3. _____

4. _____

Agency _____

Invoice To Attn: _____
(Must Be Completed)

Address _____

City _____ **State** ___ **Zip** _____

Email _____

Phone _____

Fax _____