MPD Academy

Cryptocurrency Investigations

Purpose:
This course is designed for attendees to understand why there must be a balance between Electronic and Human Intelligence in cryptocurrency investigations. Too much illicit value is being left behind. Cryptocurrency moves at the speed of the internet, and you should too. This course will teach boots on the ground law enforcement up to a federal prosecutor to recognize and seize cryptocurrency in the field. Judicial personnel must understand what you need and why. At least one attendee in each course since March 2019 has recognized something missed in a previous search or realized they had a device already in evidence that held accessible cryptocurrency.

1. Field agents, (be they local, state, or federal) do not in general, possess the knowledge to immediately recognize, identify, target and potentially sweep illicit value to safety in the field. With this course, field agents will become exponentially better sources of crypto information on an SSE (Sensitive Site Exploitation) site and gain the capability of highlighting and shaping information passed on to cyber and forensic personnel.

2. This course will also cover basic Darknet investigative techniques.

3. Upon leaving this course, all attendees will be able to materially contribute to or lead a cryptocurrency investigation.

Description:
This course will consist of three days (24 hours equivalent) of training.

The course will cover all the objectives listed below. All practical exercises will involve actual coin transactions conducted and analyzed by attendees. Exploitation of phones, computers and coin hardware storage devices will also be executed by attendees as well as hands on use of Linux, Windows and Chrome and TAILS operating systems. **Note: It is important that each attendee bring a laptop computer where you have the administrator rights (for specialized software install) and no internet filters whatsoever. USB ports should be set to active. Attendees should have permissions to install apps on phones. Attendees are encouraged to bring their own Wi-Fi hubs to reduce bandwidth draw during transactions. Personal equipment is authorized but only recommended if no PII is on the device. An old personal or agency computer that has been reset is ideal for use in this course. Bring an empty USB drive of at least 16GB for TAILS.**

Note: FOLLOWING THIS COURSE, NEVER CONNECT THE COMPUTER YOU USE IN THE COURSE TO GOVERNMENT NETWORKS WITHOUT EXPRESS CONSENT FROM YOUR RESPECTIVE IT MANAGER.

Course Objectives:

1. The basics of Bitcoin and other popular coins.
2. Coin wallets & exchange services.
3. Using smart blockchain explorers in the field to run discovered coin addresses forward and backward.
4. Google Dorking to find a transaction on the blockchain quickly from as little as one data point.
5. Transacting with subjects (suspects) or machines to analyze their coin transactions.
6. Creating alerts to monitor specific coin address activity.
7. Pseudo anonymous vs. anonymous coins.
8. Coin hard forks. They can still be relevant in older wallets.
9. How to discover crypto resources in your operational area using publicly available resources.
10. The evolution of Coin ATMs and why it has never been more important.
11. How to create, receive and spend coin from select paper wallets requiring zero identity.
12. How to convert one coin to another using decentralized conversion platforms requiring zero identity.
13. Our recommended phone app for sweeping funds in the field should you discover one.
14. Conducting hands on exploits of coin hardware storage devices.
15. Splicing in a power supply to keep a bad guy hard drive alive for exploitation. A Faraday bag lacks a very key component.
16. Coin debit cards. This is an ever-changing and important landscape.
17. Cell phone top up and crypto. An entire network of phones can be refilled from a single location, 24/7.
18. Building and improving a cryptocurrency SSE checklist.
19. Understanding how Decentralized Exchanges and Non-Fungible Tokens are used in the drug trade.
20. You found a seed and no device, learn how to look inside.
21. You found a device and no pin, passphrase or seed, information may still be accessible.
22. Developing and coordinating a cryptocurrency policy within your department, agency or task force.
23. Practical Exercises with be used throughout the training to gauge participation and proficiency.

This course is taught by William Sparks, Third Party Resources, Inc., www.3princ.com

Cryptocurrency Course

This a free course on Cryptocurrency .

Date: May 22, 23 and 24, 2023

Time: 08:30 to 16:30 (Monday & Tuesday) 08:30 to 14:30 (Wednesday)

Location:

MPD Academy

4665 Blue Plains Drive SW

Washington, D.C.

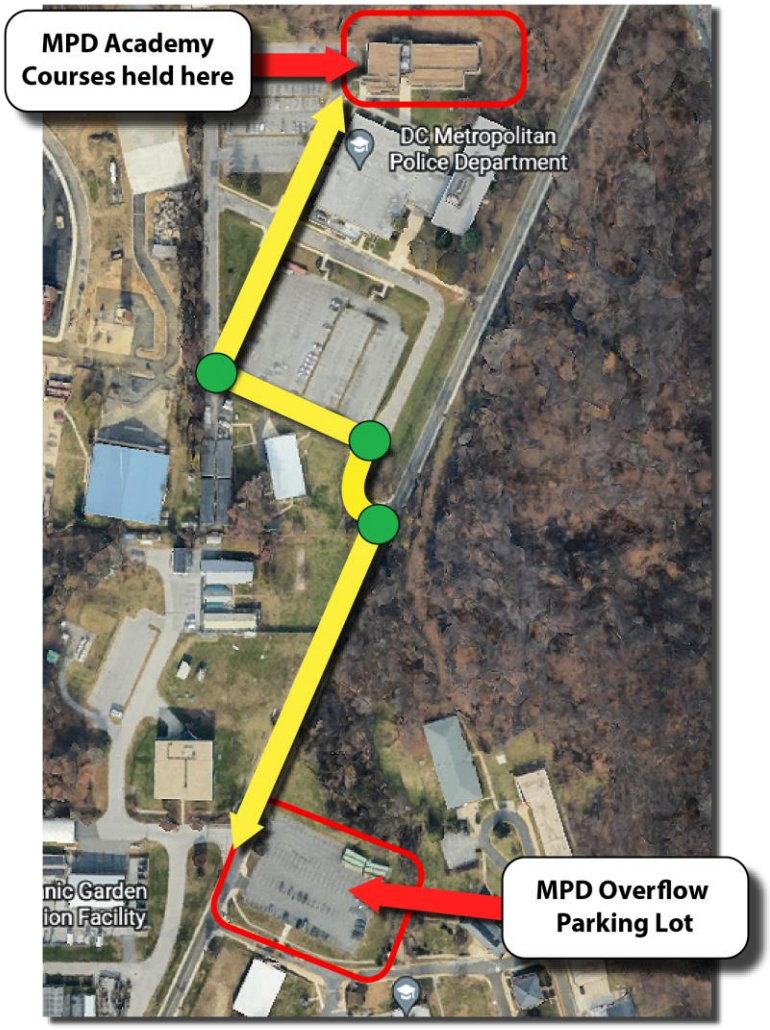
If you need to cancel please use the NHAC/HOTTS registration site to do it.

Questions:
Ramona Boland
Training Program Manager
Training Unit
Washington/Baltimore HIDTA
Serving the District of Columbia, Maryland, Virginia, and West Virginia
T- 443-980-8182 F- 301-489-1745
RBoland@wb.hidta.org

To register:
Online Registration in HOTT is as follows:

Open your web browser to https://www.nhac.org/hidtatrainingcalendar/events/27
Select ***(course name)***. Select register
Fill in the **HOTT Online Application** and select **Complete Registration**

Parking



MPD Overflow Parking Lot

*Due to the limited parking at the Academy site, they have requested that all non-MPD Officers Park at the MPD overflow Lot. This lot is about a D.C. city block from the MPD Academy.

Questions:

Ramona Boland
Training Program Manager
Training Unit
Washington/Baltimore HIDTA
T- 443-980-8182
RBoland@wb.hidta.org

Instructor Qualifications (documented):

- Has directly aided law enforcement in the successful seizure or recovery of cryptocurrency in the past 2 months.
- Has directly aided law enforcement in cryptocurrency investigations that led to arrests in the past 2 months.
- Has directly aided local law enforcement in the liquidation of seized cryptocurrency assets in the past 3 years.
- Trained approximately 1,000 LE and Military Special Ops personnel in 2022.

The Capstone exercise (day 3) will flex all subjects taught during the course. In this exercise, **the instructor will provide the following devices** for attendees to exploit for all information useful in their investigation and search as listed below:

- **Computers:** Windows, Linux, Chrome Operating System, TAILS
- **Projectors:** presentation and PICO projectors will be used throughout to increase visibility for attendees.
- **Browsers:** Chrome, Edge, Firefox, Epic, Brave, Tor, etc.
- **Phones:** iPhone and Android will be exploited during the capstone exercise.
- **Coin Hardware Devices:** Trezor, Ledger, KeepKey
- **Search Engines:** Google, Brave, Duck Duck Go, Epic, Yahoo, etc.

The Capstone review will also consist of teams comparing what they each found and finding intersecting data that would link individuals or illicit networks.

Attendees are encouraged to bring crypto case files they are working for instructor input and class collaboration in generic terms that will not compromise an investigation.

Course Agenda: Cryptocurrency Investigations

Note: the course flow will vary based on attendee understanding. Overall time will not change.

Day 1:	**08:00**	**"Firehose Day"**
20 minutes	Welcome and Admin Announcements from Wash-Baltimore HIDTA and 3PR.	
1-hour	Introduction to cryptocurrency basics.	
45 minutes	Intro to Blockchains, block explorers and practical exercise.	
45 minutes	Blockchain Transactions Visualizers (you will use those of your choice throughout).	
40 minutes	Global crypto and blockchain use cases.	
Lunch	**11:30 - 12:30**	
45 minutes	Crypto not so basics (understanding why blockchain analytics can matter in the field).	
30 minutes	Running a known bad guy using only a blockchain (practical exercise).	
1-hour	Analyzing Decentralized Exchange Transactions (these require zero identity to transact).	
1-hour	Transacting with individuals and entities to analyze them (practical exercise).	
45 minutes	Creating paper wallets to fully understand sending, receiving and sweeping of cryptocurrency.	
30 minutes	Day 1 review, quick briefing on phone app to be used.	
End Day 1	**17:00**	

Day 2	**08:00**

45 minutes	Understanding etherscan.io and all tokens that run on the Ethereum blockchain
1.75 hours	Software and Desktop wallets you may encounter or create to use (practical exercise)
1.0 hour	Crypto phone app and paper wallet practical exercises
Lunch	**11:30 – 12:30**
1.0 hours	Darknet basics, accessing it, paste bins, indexes, screen names, markets, etc.
1.5 hours	TAILS, can be quirky and unusual to setup initially but you gotta know it.
1.5 hours	Popular Desktop and Software wallets that bad guys and you can use.
30 minutes	Making software and desktop wallets secure (practical exercise).
End Day 2	**17:00**

Day 3	**08:00**
30 minutes	Virtual machine software, remote access software, kill switches.
30 minutes	Keeping power to a bad guy computer. (Why? Bitlocker, hard keys, bad battery, encrypted drives).
30 minutes	Material review and final setup for Capstone

The capstone exercise typically takes 2.5 to 4 hours to complete depending on class proficiency.

Lunch	**12:00 – 13:00** (attendees may elect to work through lunch)
2.5 to 4 hours	Capstone Exercise
30 minutes	Completion of post course review, turn over to Wash-Baltimore HIDTA Staff

End of Course **17:00** In the event the Capstone Exercise completes before 1700, the instructor will stay on through COB to conduct additional team or individual training as requested. Typically, a group of 5-8 will stay on to repeat particular tasks or more importantly, they take guidance on actual cases they are working on. That will continue to a time TBD. This is where most one-to-one training takes place.

Two computers will be running in the classroom for attendee use during the entire course for:

1) Public breach database. This has been 100% successful in advancing cases.
2) Subscription block explorer. This often advances cases.

You have reach back capabilities with this course at no cost. We have LE personnel contact us that attended years ago, and we help every one of them. We will not try to sell you any software, subscription service or hardware.

What a few former attendees said about the course:

What were the strong points of this course? (Houston HIDTA 2022)

- *"Hands on training and how to develop cases."*
- *"Working in small groups on the hands-on exercises was great, especially in a class this size and with both LE and bankers. Overall - wonderful!"*
- *"Instructor provided great practical exercises."*
- *"It was a great class. I like the fact that bankers were invited. This gives them an understanding of what law enforcement are dealing with."*
- *"It was one of the better trainings I've had in an almost 20-year career. Extremely helpful."* FBI SA

Northern California HIDTA 2022

- *"The hands on portion of the class. I was able to present a case I needed help with and received direction."*
- *"Hands on software and practical exercises"*
- *"Great visual aids and learning techniques with hands on experience."*
- *"The information was amazing. I thought all of the course information was very relevant. This class was extremely helpful for me and I wish I had taken it sooner."*
- *"The instructor attempted to communicate with all investigators at every cryptocurrency experience level (beginner to advance)."*
- *"The hands on stuff-creating a paper wallet, trading crypto, and then breaking into the laptops , phones and thumb drives."*