Practical Cryptocurrency Investigations Course Outline

Presenter: ESTOC Advisors Principal – Jason Tucker, CPA, CFF, CCE
Format: 16-Hour Hands-On Investigation Workshop

Prerequisites: Students should possess a basic understanding of cryptocurrency concepts, wallets, exchanges, and blockchain terminology.

Course Description

This advanced hands on workshop teaches investigators how to identify, preserve, analyze, and investigate cryptocurrency evidence using real blockchain data, practical investigative techniques, and live investigative exercises.

To support realistic hands on training in a safe environment, ESTOC has developed and launched ESTOC Training Token (EXT), a custom Law Enforcement only training asset used exclusively for live course exercises. EXT allows students to perform real cryptocurrency transactions, transfers, swaps, and tracing exercises during class without risking real capital or using market traded assets.

ESTOC will also provide each student with a custom hardware training wallet for use during the course, which students will keep at no additional cost. Together, the ESTOC training token and hardware wallets create a controlled learning environment where students can safely experience real blockchain transactions while building practical investigative confidence.

Target Audience

- Criminal Investigations Division (CID)
- Financial & White-Collar Crimes
- Narcotics Investigations
- Organized Crime
- Intelligence / Analyst Personnel supporting investigations

Materials Provided

- Course Material Handout
- Investigation Worksheet (Excel file)
- Crypto Hardware Wallet (ESTOC NFC Wallet)
- 50,000 ESTOC (EXT) Custom LE Training Tokens
- Crypto Service Reference Sheet: including CEX, Wallets, ATMs, Off-Ramps, etc.

Day One – Investigating Existing Activity

Day One Focus: Students investigate cryptocurrency activity that has already occurred by identifying transactions, tracing funds, developing attribution leads, and documenting findings from real blockchain evidence.

Session 1 – Investigative Foundations & Tool Setup

Duration: 60 Minutes

Description
Students establish training wallets, become familiar with blockchain explorers, and learn the investigative workflow and documentation process used throughout the course.

Learning Objectives

- Configure training wallets and learn the role of each to be used during the course
- Understand wallet addresses, QR codes, and blockchain transaction identifiers
- Understand the basic workflow for using blockchain explorers during an investigation
- Establish documentation procedures and evidence worksheet expectations
- Recognize the difference between course setup activities and investigative activities

Practical Exercise

- Install and configure training wallets
- Receive burner card wallet and training assets
- Review wallet addresses, QR codes, and explorer pages

Session 2 – Evolution One: Find the Transaction

Duration: 60 Minutes

Description
Students identify and document a cryptocurrency transaction using a provided wallet address and blockchain explorer.

Learning Objectives

- Locate a transaction using a wallet address
- Identify key transaction details including TXID, amount, date, and counterparties
- Recognize how transaction evidence appears on a blockchain explorer
- Document transaction evidence in an investigative format

Practical Exercise

- Locate a target transaction on-chain and Identify key transaction details
- Complete an evidence worksheet documenting the transaction

Session 3 – Evolution Two: Follow the Funds

Duration: 75 Minutes

Description
Students trace cryptocurrency through multiple wallets to identify transaction flow, current destination, and investigative leads.

Learning Objectives

- Trace funds across multiple wallets and transactions
- Identify transaction chains and wallet relationships
- Recognize labels, services, and potential destination wallets
- Document movement of funds in an organized evidence format

Practical Exercise

- Trace a transaction through multiple wallet hops
- Identify current location of funds and relevant counterparties
- Record findings and transaction flow in an evidence table

Session 4 – Evolution Three: Wallet Hunting

Duration: 75 Minutes

Description
Students develop cryptocurrency leads using usernames, email addresses, forum posts, and open-source intelligence techniques.

Learning Objectives

- Identify attribution opportunities outside the blockchain
- Conduct targeted OSINT to support a cryptocurrency investigation
- Associate online identifiers with potential wallet activity
- Develop investigative leads when no wallet address is initially known

Practical Exercise

- Review provided online identifiers and artifacts
- Conduct targeted OSINT and Identify wallet leads or crypto-related service usage
- Document attribution findings and supporting evidence

Session 5 – Evolution Four: The Empty Wallet

Duration: 60 Minutes

Description
Students investigate a wallet with little or no current balance and reconstruct historical activity to identify prior transactions, token movement, and associated wallets.

Learning Objectives

- Investigate wallets with no current balance rather than treating them as dead ends
- Review historical wallet activity and token transfer history
- Identify prior counterparties and associated wallets
- Develop investigative leads from historical blockchain activity

Practical Exercise

- Review a wallet with zero or near-zero current balance
- Reconstruct historical wallet and token activity
- Identify prior transactions, transfers, and associated wallets
- Complete evidence documentation of findings

Session 6 – Evolution Five: NFT Attribution

Duration: 60 Minutes

Description
Students use NFTs and related blockchain artifacts to develop attribution leads and connect wallet activity to marketplace or user information.

Learning Objectives

- Recognize NFTs and blockchain artifacts as investigative evidence
- Identify alternate attribution opportunities beyond simple wallet tracing
- Use marketplace or platform artifacts to develop suspect leads
- Document how a blockchain artifact supports attribution

Practical Exercise

- Review a wallet containing an NFT or related artifact
- Identify the associated marketplace or platform
- Develop attribution leads from the artifact
- Document findings and investigative relevance

Session 7 – Evolution Six: Gas Source & Off-Chain Lead Development

Duration: 60 Minutes

Description
Students trace gas funding and exchange-related activity to identify off-chain investigative leads, including potential subpoena opportunities.

Learning Objectives

- Identify the significance of gas funding in cryptocurrency investigations
- Trace ETH or other gas funding to likely source wallets or services
- Recognize exchange interactions and potential off-ramp behavior
- Identify potential off-chain investigative leads and subpoena targets

Practical Exercise

- Review a wallet with limited direct evidence
- Trace gas funding or related blockchain support activity
- Identify likely exchange interaction or service provider involvement
- Document investigative leads and next-step opportunities

End of Day One - Q&A

Day Two – Creating Activity, Then Investigating It

Day Two Focus: Students perform live cryptocurrency transactions, swaps, and cash-out activity using training assets, then investigate the resulting blockchain evidence and complete progressively more complex practical exercises.

Session 8 – Evolution Seven: Basic Wallet Transactions

Duration: 75 Minutes

Description
Students perform basic wallet-to-wallet cryptocurrency transactions using their course wallets and training assets, then verify and document the resulting blockchain activity.

Learning Objectives

- Conduct basic wallet-to-wallet cryptocurrency transfers
- Recognize how sent and received transactions appear in wallets and explorers
- Build confidence using wallet interfaces before moving into more advanced transactions

Practical Exercise

- Send training assets between the student's mobile wallet and burner card wallet
- Complete one or more transfers between teammates within the same group
- Verify balances, transaction history, and explorer results
- Document completed transactions and resulting wallet changes

---

Session 9 – Evolution Eight: Token Swap

Duration: 75 Minutes

Description
Students complete a live token swap using ESTOC training assets and then review the resulting approval, smart contract, and token transfer activity on-chain.

Learning Objectives

- Understand token approvals and decentralized exchange interactions
- Complete a token swap using a training wallet
- Identify approval transactions, swap activity, and resulting token transfers
- Distinguish swap activity from a basic wallet-to-wallet transfer

Practical Exercise

- Complete an EXT to EUSD swap
- Review the resulting on-chain activity and contract interactions
- Document the transaction sequence and key findings

Session 10 – Evolution Nine: Exchange Cash-Out

Duration: 60 Minutes

Description
Students transfer training assets to a designated exchange deposit wallet to demonstrate cash-out behavior and identify how off-ramp activity appears on-chain.

Learning Objectives

- Understand how exchange cash-out activity appears on-chain
- Recognize exchange deposit behavior and off-ramp indicators
- Connect wallet funding, swap activity, and exchange deposit activity into one investigative chain
- Identify potential legal process or subpoena opportunities arising from exchange use

Practical Exercise

- Transfer designated training assets to a provided exchange deposit wallet
- Review the resulting blockchain transaction and destination wallet activity
- Identify the significance of the transaction from an investigative perspective
- Document the transaction as part of an off-ramp scenario

Session 11 – Evolution Ten: Swaps, Laundering & Financial Movement

Duration: 90 Minutes

Description
Students investigate more complex value movement involving wallet-to-wallet transfers, swaps, and multi-step activity designed to obscure the flow of funds.

Learning Objectives

- Trace value across multiple wallets and asset types
- Identify movement patterns commonly associated with laundering or obfuscation
- Distinguish between simple transfers and layered financial movement
- Document multi-step transaction activity in an organized investigative format

Practical Exercise

- Review a scenario involving transfers, swaps, and layered movement
- Trace value through multiple transactions and wallets
- Identify laundering indicators or complexity indicators
- Complete evidence documentation of the movement and investigative findings

---

Session 12 – Final Evolution: Red Team / Blue Team Capstone Investigation

Duration: 150 Minutes

Description
Students participate in a full capstone exercise in which one team creates cryptocurrency activity and another team investigates it, applying the full range of skills learned throughout the course.

Learning Objectives

- Conduct an end-to-end investigation using course concepts and tools
- Investigate transactions, wallet activity, swaps, and cash-out behavior created by another team
- Develop investigative findings, attribution leads, and evidence documentation
- Prepare and present a concise investigative summary of conclusions

Practical Exercise

- Review another team's wallet activity, transfers, swaps, and cash-out behavior
- Trace and document the relevant blockchain activity
- Develop an investigative summary and supporting evidence package
- Participate in team debrief and presentation of findings

End of Day Two - Q&A