c4 Academy

CRYPTOCURRENCY CRIME CONTROL & COMPLIANCE

www.c4academy.com. team@c4academy.com

The challenge of cryptocurrency crime

Crypto crime is a multi-billion-dollar global problem: rug pulls, pump-and-dumps, ransomware, frauds, smart contract attacks, hacks, wash trading, and more.

To make things worse, cryptocurrencies now sit at the centre of global money laundering, terrorism financing, darknet market activity, drug and weapons trafficking, human trafficking, migrant smuggling, organised cybercrime, illegal gambling, counterfeit goods, wildlife smuggling, sanctions evasion, tax evasion, and unlicensed money transmission.

A RAND study with the National Institute of Justice and the Police Executive Research Forum found major capability gaps in how U.S. law enforcement handles cryptocurrency-related crime.

The report highlights fragmented jurisdiction, limited training, and unclear evidence-handling protocols as key weaknesses.

"Cryptocurrency Crime is Evolving. Investigators Must Evolve Faster."

Among 24 critical needs identified, top priorities included standardized procedures for seizing and securing crypto assets, two-person verification controls, expanded practitioner training, and stronger inter-agency information sharing.

The study also noted that most small and mid-sized agencies lack access to effective blockchain-tracing tools, and that even open-source solutions require technical expertise and infrastructure beyond the reach of many departments.

Cryptocurrency Crime Analyst

A c4 certified Cryptocurrency Crime Analyst (CCA) works at the intersection of technology, finance, and law enforcement. The role spans the full investigative lifecycle:

1. Detecting early red flags in wallets, transactions, platforms & communications.

2. Tracing illicit fund flows across blockchains, exchanges, and bridges.

3. Linking technical evidence to real-world actors.

4. Preserving evidence during live investigations and seizures.

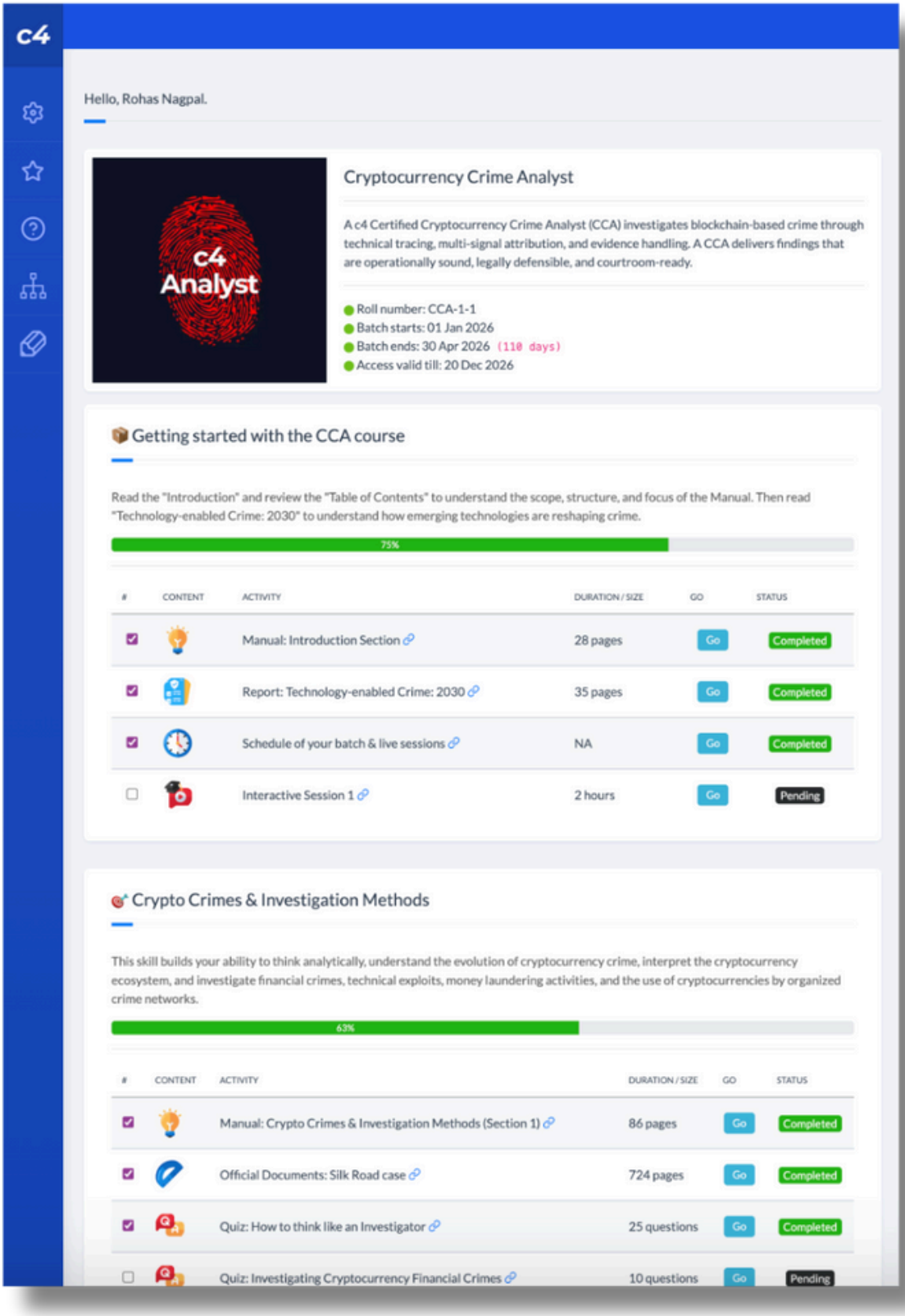
5. Translating complex blockchain activity into defensible legal narratives.

The CCA program is designed for:

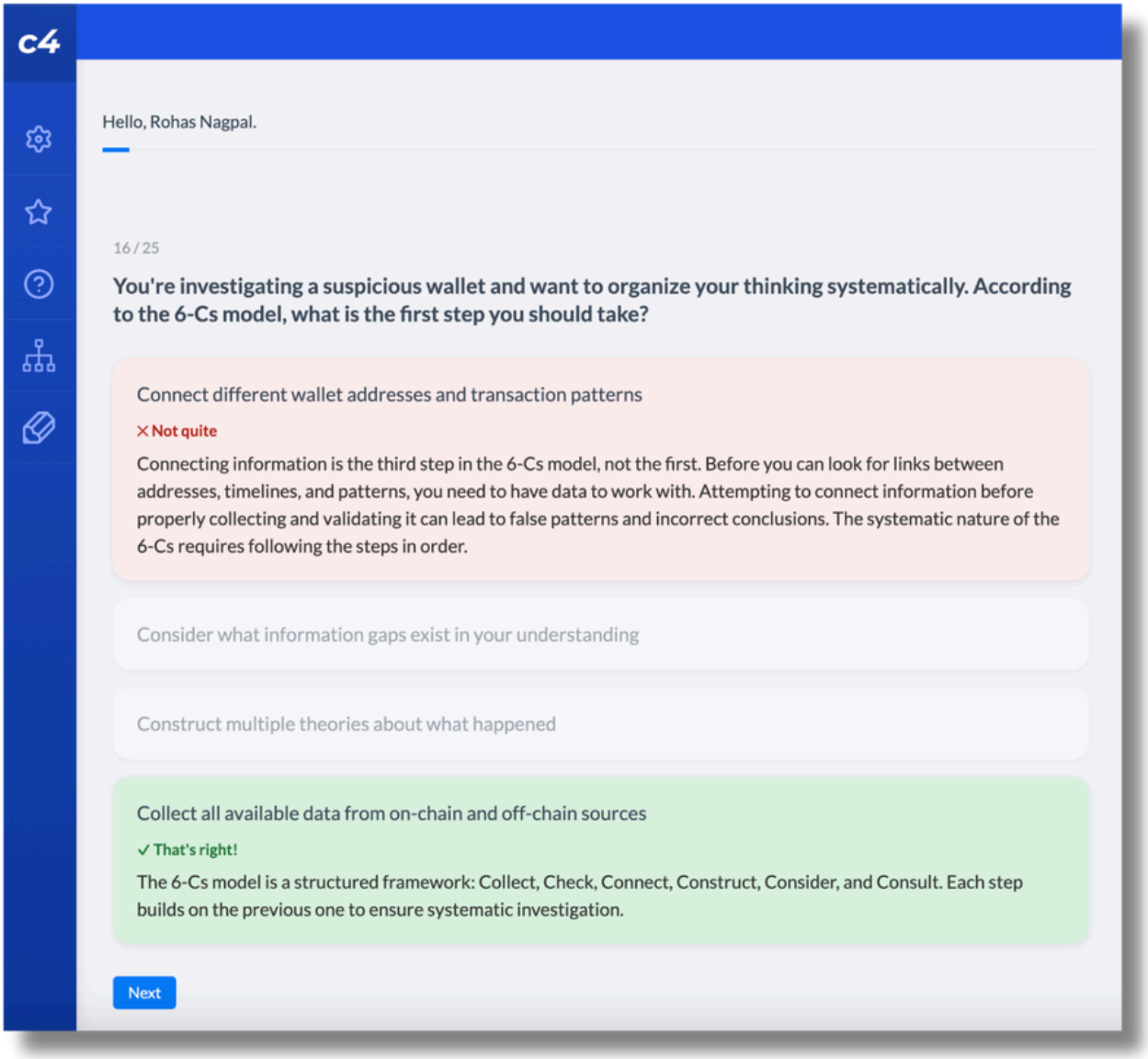
- Police & Tax Officers
- VASP Teams
- Blockchain & Web3 Developers
- Cybercrime Investigators
- Fintech & Finance Professionals
- Compliance, AML & Risk Professionals
- Cyber Security Professionals
- Fraud-Risk Teams
- PIs & Insurance-Fraud Examiners
- CAs, CPAs & Forensic Auditors
- Lawyers & Legal Counsels
- Technology Professionals
- Engineering Students

Fees (India): INR 45,000 + GST
Fees (International): US$ 699
Group discounts & Govt. pricing available.

The CCA course is built around the
Cryptocurrency Investigation & Forensics Manual by Rohas Nagpal.
It's an operational field guide full of checklists, SOPs, and best practices.



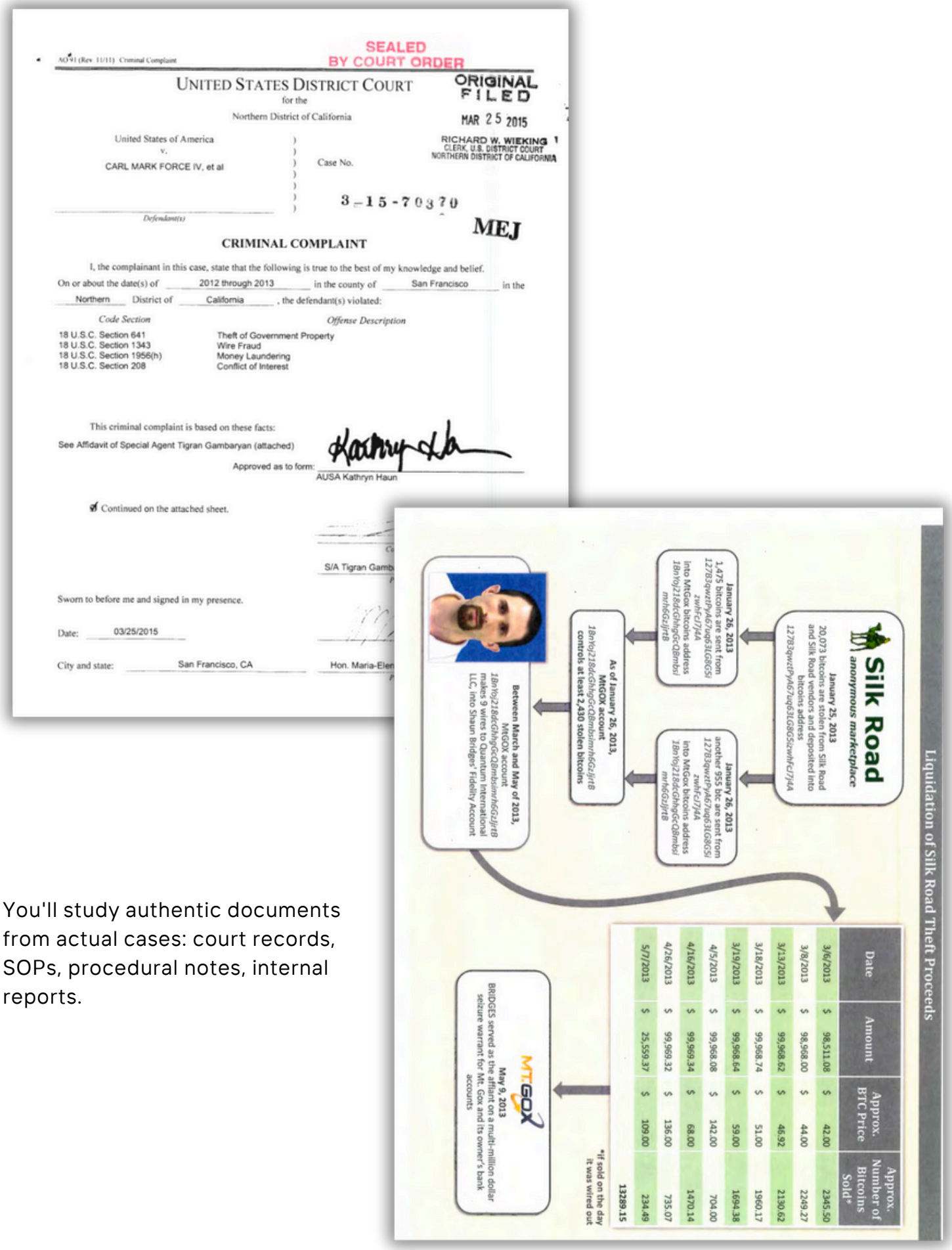
The **c4 LEARN** digital platform powers the CCA course with Interactive Quizzes, Deep-dive Videos, Court Records, and Official Documents.



Every **c4 Interactive Quiz** is designed to teach, not just test.

Every answer - right or wrong - includes a detailed explanation that shows you the logic behind it, the common mistakes it represents, and how it maps to real investigative thinking.

You're not just answering, you're learning to think.



SEALED
BY COURT ORDER

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT
for the
Northern District of California

ORIGINAL
FILED
MAR 25 2015
RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

United States of America
v.
CARL MARK FORCE IV, et al
Defendant(s)

Case No.
3-15-70370
MEJ

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 2012 through 2013 in the county of San Francisco in the Northern District of California, the defendant(s) violated:

Code Section	Offense Description
18 U.S.C. Section 641	Theft of Government Property
18 U.S.C. Section 1343	Wire Fraud
18 U.S.C. Section 1956(h)	Money Laundering
18 U.S.C. Section 208	Conflict of Interest

This criminal complaint is based on these facts:

See Affidavit of Special Agent Tigran Gambaryan (attached)

Approved as to form: AUSA Kathryn Haun

Continued on the attached sheet.

S/A Tigran Gamb

Sworn to before me and signed in my presence.

Date: 03/25/2015

City and state: San Francisco, CA

Hon. Maria-Elen

Silk Road
anonymous marketplace

January 25, 2013
20,073 bitcoins are stolen from Silk Road and Silk Road vendors and deposited into bitcoins address
12783qwztPyA67uqG3LG8GSzwhFcJ7j4A

January 26, 2013
1,475 bitcoins are sent from 12783qwztPyA67uqG3LG8GSzwhFcJ7j4A into MtGox bitcoins address 18n9oj218dcGhhgGcQBmbsimrh6GzJjrtB

January 26, 2013
another 955 btc are sent from 12783qwztPyA67uqG3LG8GSzwhFcJ7j4A into MtGox bitcoins address 18n9oj218dcGhhgGcQBmbsimrh6GzJjrtB

As of January 26, 2013, MtGOX account 18n9oj218dcGhhgGcQBmbsimrh6GzJjrtB controls at least 2,430 stolen bitcoins

Between March and May of 2013, MtGOX account 18n9oj218dcGhhgGcQBmbsimrh6GzJjrtB makes 9 wires to Quantum International LLC, into Shaun Bridges' Fidelity Account

Liquidation of Silk Road Theft Proceeds

Date	Amount	Approx. BTC Price	Approx. Number of Bitcoins Sold*
3/6/2013	$ 98,511.08	$ 42.00	2345.50
3/8/2013	$ 98,968.00	$ 44.00	2249.27
3/13/2013	$ 99,968.62	$ 46.92	2130.62
3/18/2013	$ 99,968.74	$ 51.00	1960.17
3/19/2013	$ 99,968.64	$ 59.00	1694.38
4/5/2013	$ 99,968.08	$ 142.00	704.00
4/16/2013	$ 99,969.34	$ 68.00	1470.14
4/26/2013	$ 99,969.32	$ 136.00	735.07
5/7/2013	$ 25,559.37	$ 109.00	234.49
			13289.15

*if sold on the day it was wired out

MT.GOX

May 9, 2013
BRIDGES served as the affiant on a multi-million dollar seizure warrant for Mt. Gox and its owner's bank accounts

You'll study authentic documents from actual cases: court records, SOPs, procedural notes, internal reports.

Get Hands-On with Real Cryptocurrencies

c4 LEARN lives on the Polygon Mainnet and has a total supply of 21 million. You can view its details and smart contract on Polygonscan: https://polygonscan.com/token/0x5C1874bcb8Dc2b581B4Ee2776A5A32a44ea2881B

c4 USD lives on the Polygon Mainnet and has a total supply of 1 trillion. You can view its details and smart contract on Polygonscan: https://polygonscan.com/token/0x831490d955a5168f44d104173bfd72573b92efea

The LEARN / USD tokens can be swapped on QuickSwap: https://dapp.quickswap.exchange/swap/v3/0x831490D955A5168f44d104173BFd72573b92EfeA/0x5C1874bcb8Dc2b581B4Ee2776A5A32a44ea2881B?chainId=137

c4 JPY lives on the Polygon Mainnet and has a total supply of 1 trillion. You can view its details and smart contract on Polygonscan.

c4 case studies are not made-up examples. They are drawn from real cryptocurrency crime investigations.

c4 Crypto Crime Challenge 1:
The Zimblia Infiltration

Intelligence agencies have intercepted credible signals that a newly formed international organized crime syndicate is attempting to establish a foothold in Zimblia, a wealthy island nation known for its lax financial oversight and strategic location.

Preliminary estimates suggest that over USD 500,000 is being funneled into Zimblia to recruit and consolidate local criminal networks. The funds are believed to be intended as onboarding payments, operational capital, and loyalty incentives.

Local law enforcement has arrested Cyrus, a well-known criminal fixer with deep ties to smugglers, document forgers, and corrupt intermediaries. Cyrus was carrying a brand new mobile phone.

An extensive forensic analysis of this phone (covering call logs, messaging apps, cloud backups, and deleted data), revealed just 1 image that had been deleted an hour before his arrest.

Your mission, should you choose to accept it, is to analyze the image and determine if it supports the hypothesis of syndicate expansion into Zimblia.

You can download the image from here: https://c4academy.com/challenges/1/1000501223.jpg

Syllabus

Skill 1. Cryptocurrency Wallet Forensics

Extracting, analyzing, and attributing cryptocurrency wallets to trace digital assets & link them to real-world identities.

1. Wallet Fundamentals
2. Blockchain Explorers
3. Forensic Investigation of Wallets
4. Seizure Protocols & Evidence Handling
5. Linking Wallets to Real-World Identities

Skill 2. Technology Fundamentals for Investigators

Understanding data structures that underpin crypto currency systems

1. Blockchain Technology
2. Smart Contracts
3. Token Standards
4. Internet & Web Technology
5. On-Chain & Off-Chain Data

Skill 3. Investigating Cryptocurrency Crimes

1. How to Think Like an Investigator
2. Silk Road: The crime that changed investigation forever
3. Early Bitcoin Thefts & Exchange Hacks
4. Ponzi Schemes & Scams
5. Ransomware & Malware
6. DeFi Exploits
7. Darknet Markets & Illicit Trade
8. Social Engineering, Identity Exploits & Other Crimes
9. The Cryptocurrency Ecosystem
10. Investigating Cryptocurrency Financial Crimes
11. Investigating Technical Exploits in Cryptocurrency Protocols
12. Investigating Cryptocurrency-Enabled Money Laundering
13. Investigating Cryptocurrency Use in Organized Crime

Skill 4. Investigating Blockchain Ecosystems

1. Crypto Assets and Instruments
2. Investigating Bitcoin Ecosystem
3. Investigating the EVM Ecosystem
4. Investigating the Tron Ecosystem
5. Investigating Binance Ecosystem
6. Investigating the Solana Ecosystem
7. Investigating Privacy Coins
8. Investigating Stablecoins
9. Investigating Centralized Exchanges
10. Investigating Decentralized Exchanges
11. Investigating the DeFi Ecosystem
12. Freezable Tokens and Chain Controls

Skill 5. Investigating Digital Anonymity & Covert Infrastructure

1. Investigating Parallel Internets
2. Investigating Messaging Platforms
3. Email Investigation
4. Investigating Decentralized Hosting & Storage Protocols
5. Investigating Decentralized Domains
6. Handling Encrypted & Obfuscated Data

Skill 6. Field Operations & Cryptocurrency Crime Scenes

1. Identifying and Classifying Cryptocurrency Evidence
2. Device Seizure, Volatile State Preservation, and Key Material Handling
3. Digital Asset Seizure Documentation & On-Site Coordination

Skill 7. Digital Evidence & Legal Processes

1. Lawful Authority and Jurisdiction
2. Evidence Handling and Admissibility
3. Courtroom Communication and Narrative
4. Expert Witness Strategy and Counter-Forensics
5. Data Governance, Custody, and Asset Control
6. Case Coordination and Investigative Integrity

C4 Academy Partner Ecosystem

c4 Academy is building a structured, scalable, global partner ecosystem to expand high-quality cryptocurrency investigation education. The ecosystem is organized across 4 clearly defined partner roles, each aligned to a specific function in the learning and delivery lifecycle.

1. Career Advisors

Career Advisors are experienced professors, academic mentors, and industry practitioners who guide prospective students in understanding careers in cryptocurrency investigation and blockchain forensics.

Their role is purely advisory. They help learners assess whether the field aligns with their background, career stage, and long-term goals, and explain how c4 Academy's programs fit into professional pathways across law enforcement, compliance, cybersecurity, and financial investigations.

Career Advisors act as trusted bridges between academia, industry, and students. They do not conduct marketing or sales activities, nor do they deliver training.

- Earn a commission for every successful admission referred.
- No financial investment or infrastructure required.
- Ideal for educators, senior professionals, and mentors with credibility & reach.

2. Certified Trainers

Certified Trainers are subject-matter professionals authorized to deliver c4 Academy's courses to learners across government, private sector, and academic settings. All trainers must undergo a formal trainer-certification process conducted by c4 Academy. This includes:

- Deep alignment with C4 Academy’s curriculum and investigation frameworks.
- Training on instructional design, teaching methodology, and assessment.
- Calibration on case-based learning, legal accuracy, and evidentiary rigor.

3. Authorised Training Centers (ATCs)

Authorised Training Centers (ATCs) are institutional partners that deliver c4 Academy programs at scale across regions and jurisdictions. These partners serve as the physical and operational backbone of c4 Academy's training ecosystem.

ATCs are responsible for establishing and maintaining dedicated training infrastructure in line with C4 Academy’s standards, including classrooms, labs, secure systems, and administrative support. They also manage local operations such as scheduling, student coordination, and on-ground logistics, while academic content, curriculum control, and certification remain centrally governed by c4 Academy.

ATCs benefit from access to c4 Academy's globally relevant curriculum, brand, certification framework, and expert network, enabling them to offer specialized, high-demand programs in cryptocurrency investigation and digital financial crime.

4. Empanelled Investigators

Empanelled Investigators are seasoned professionals with proven expertise in cryptocurrency investigations, blockchain forensics, and digital asset tracing. These investigators are engaged by c4 Academy on a case-specific or project basis to support:

- Law enforcement investigations
- Corporate and financial institution probes
- Internal fraud, AML, and compliance cases
- Training case development and expert consultations

Empanelment is granted only after a rigorous evaluation of technical competence, investigative experience, and legal understanding. Empanelled Investigators may be called upon to independently handle cases, collaborate with agencies, or mentor advanced trainees on real-world investigations.

Team c4

Rohas Nagpal

Author, lawyer & investigator with 25+ years of experience, Rohas has worked across 18 countries on complex cases involving digital forensics, cyber terrorism, financial crime, and corporate liability. He co-founded the Asian School of Cyber Laws in 1999 and has advised the Government of India on rule-making under Information Technology Act.

He has authored several books including:

- Cyber Crime Investigation Manual
- Commentary on the Information Technology Act
- Cryptocurrency Investigation & Forensics Manual
- Blockchain Engineering Playbook

Santosh Khadsare

Army veteran, TEDx speaker, and former Scientist ‘E’ at CERT-In (Ministry of Electronics & Information Technology, Government of India), with over 25 years of experience in digital forensics, cyber incident response, and national cyber defense.

He has led and advised on multiple high-impact, national-level cyber investigations, working at the intersection of tech, law enforcement, and policy.

Shinam Arora

Computer Science Engineer and technology entrepreneur with 15+ years of experience in digital evidence analysis, blockchain systems, and emerging-technology investigations.

Co-founder of BankChain, a pioneering blockchain consortium comprising 37 banks in collaboration with IBM, Microsoft, and Intel, focused on secure, enterprise-grade distributed ledger solutions.

Contact c4 Academy

Website:
www.c4academy.com

Email us:
team@c4academy.com

Chat with us:
+91-7707000003

WhatsApp Group
https://chat.whatsapp.com/GBUDWd30WscASvPu70bqfv