C4

Cryptocurrency Investigation & Blockchain Forensics

Cryptocurrency Crime is a Multi-Billion Dollar Global Problem

Rug pulls. Ransomware. Money laundering. Darknet markets. Human trafficking. Sanctions evasion. Terrorism financing.

Cryptocurrencies now sit at the centre of the world's most serious financial crimes.

Yet most investigators, compliance officers, and legal professionals lack the training, tools, and frameworks to effectively detect, trace & prosecute it.

The Scale of Cryptocurrency Crime

Cryptocurrency crime is no longer a niche problem. Global losses reached a record $17 billion in 2025. This was powered by AI-generated personas, cross-chain obfuscation, and increasingly sophisticated laundering routes.

The Capability Gap in Law Enforcement

A RAND study conducted with the US National Institute of Justice and the Police Executive Research Forum identified 24 critical capability gaps in how law enforcement handles cryptocurrency-related crime.

Top priorities include:

- standardised procedures for seizing and securing crypto assets,
- two-person verification controls,
- expanded practitioner training, and
- stronger inter-agency information sharing.

The study found 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.

Fragmented jurisdiction, limited training, and unclear evidence-handling protocols remain the defining weaknesses across the board.

Why Existing Solutions Fall Short

Most blockchain analytics providers offer powerful software — but software alone does not make an investigator. Their training is designed to teach you how to use their tool, not how to investigate cryptocurrency crime.

Investigators trained only on a vendor's platform are dependent on that vendor's data, that vendor's interface, and that vendor's continued access. When the tool changes, the skill disappears.

Compliance certifications from other providers focus heavily on AML frameworks and regulatory checklists — but leave investigators without the technical depth to trace funds across chains, analyse smart contracts, or handle evidence at a crime scene.

No single provider before c4 has combined deep investigative training, purpose-built operational tools, and a comprehensive forensics manual into one integrated program.

The c4 Solution

c4 delivers the world's most comprehensive cryptocurrency crime investigation ecosystem:

- structured certifications,
- purpose-built investigation tools, and
- a 6-volume forensics manual — all under one roof.

Training that builds real skills.
Every c4 course is built around the Cryptocurrency Investigation & Forensics Manual and delivered through:

- real case studies,
- authentic court records, interactive quizzes, and
- live expert-led sessions.

Learners don't just pass exams — they learn to think like investigators.

Tools designed for investigators.
c4's suite of investigation tools covers every phase of a cryptocurrency investigation: from seed phrase recovery and wallet forensics to smart contract analysis, DeFi monitoring, cyber attribution, and field seizure.

A manual built for the courtroom.
The Cryptocurrency Investigation & Forensics Manual is not a product guide. It is a practitioner's framework — legally grounded, operationally tested, and written to support investigations that need to hold up in court.

A global partner network.
c4's ecosystem of Career Advisors, Certified Trainers, Authorised Training Centers, and Empanelled Investigators ensures that high-quality cryptocurrency investigation capability can be deployed anywhere in the world.

Who Needs This

Cryptocurrency crime touches every part of the financial and legal system. c4 serves the full range of professionals who encounter it:

- **Law Enforcement & Government:** Police officers, cybercrime investigators, tax authorities, financial intelligence units, prosecutors, and judges who need to detect, investigate, seize, and prosecute cryptocurrency crime.

- **Compliance & Financial Crime:** AML analysts, compliance officers, VASP teams, risk professionals, and fintech firms who need to identify illicit activity, meet regulatory obligations, and protect their platforms.

- **Legal & Forensic Professionals:** Lawyers, legal counsels, chartered accountants, forensic auditors, and insurance investigators who work with cryptocurrency evidence, valuations, or disputes.

- **Technology & Web3:** Blockchain developers, smart contract auditors, Web3 security professionals, and cybersecurity teams who need investigative frameworks to complement their technical skills.

c4 Courses

- **Cryptocurrency Crime Analyst (CCA):** Comprehensive cryptocurrency crime investigation and blockchain forensics program. For details, see: https://c4academy.com/cryptocurrency-crime-analyst.php

- **Cryptocurrency Crime Investigator (CCI):** Focused, practical certification for investigators who need core blockchain tracing and wallet forensics skills — fast. For details, see: https://c4academy.com/cryptocurrency-crime-investigator.php

c4 Tools

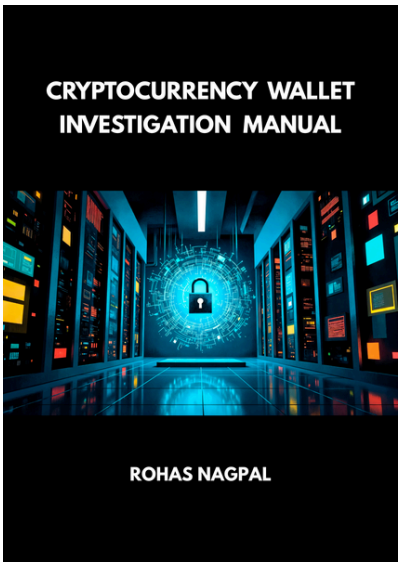
- **c4 Lab:** Cryptocurrency Investigation, Blockchain Forensics, and DeFi Monitoring platform.

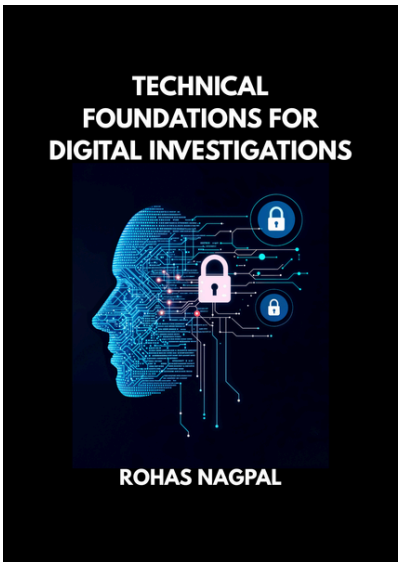
- **c4 Field:** USB-deployable forensic acquisition platform.

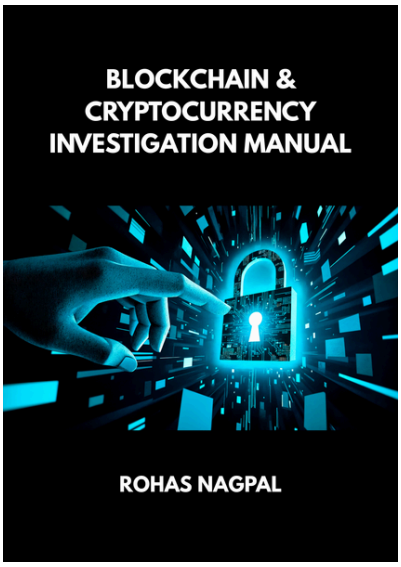
Cryptocurrency Investigation & Forensics Manual

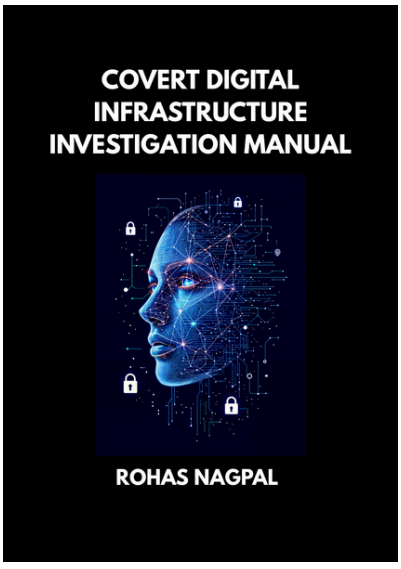
The Cryptocurrency Investigation & Forensics Manual by Rohas Nagpal is a 6-volume investigative framework covering every dimension of cryptocurrency crime — from wallet forensics to global legal enforcement. It is the backbone of every c4 certification program.

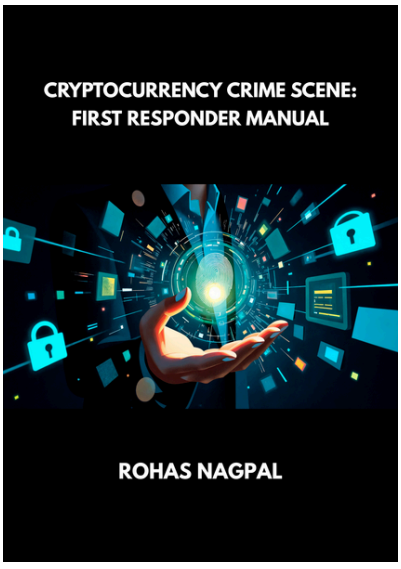
For the detailed Table of Contents of each Volume, see:
https://c4academy.com/Cryptocurrency-Investigation-Forensics-Manual.php

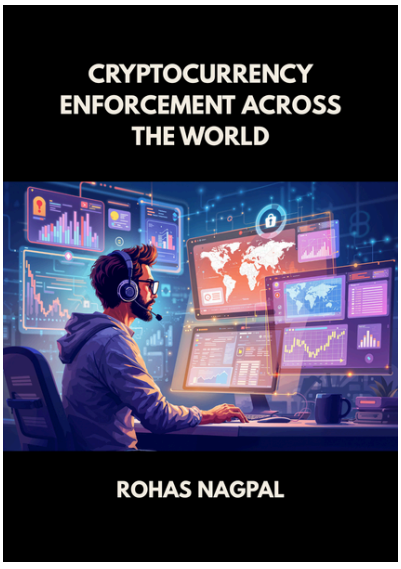












Cryptocurrency Crime Analyst

Learn to investigate cryptocurrency crime from first red flag to court-ready evidence.

Who is a Cryptocurrency Crime Analyst?

A c4 certified Cryptocurrency Crime Analyst (CCA) is a professional trained to detect, trace, attribute, and present blockchain-based criminal activity — from the first red flag to defensible evidence in court.

Think of a CCA as someone who stands at the intersection of technology, finance, and law enforcement. Not just a tech person. Not just an investigator. Both.

You are equipped to handle the full investigative lifecycle — from the moment a suspicious wallet shows up, all the way to the moment you take the stand and explain it to a judge.

The CCA certification covers six skill areas, built directly from the content of the six-volume Cryptocurrency Investigation & Forensics Manual:

6 Skills of a CCA

1. **Wallet Forensics —** You learn to identify wallets, trace ownership, and extract investigative leads from addresses, keys, and transaction histories.

2. **Technical Foundations —** You understand how blockchains actually work, so you are never fooled by technical misdirection from a suspect or their lawyer.

3. **Blockchain Tracing —** You follow the money. Across chains, across exchanges, across DeFi protocols and bridges.

4. **Covert Digital Infrastructure —** You investigate the dark web hosting, encrypted communications, and obfuscation tools that criminals use to hide their operations.

5. **Crime Scene First Response —** You know how to preserve digital evidence at the scene and maintain an airtight chain of custody.

6. **Legal Enforcement —** You navigate legal frameworks across 34 jurisdictions and prepare findings for international cooperation and court presentation.

Regular Fees

- Fees (India): INR 60,000 + GST
- Fees (International): US$ 799

Early bird discounts, group discounts, and government pricing available.

Everything Included

- 1-year access to all 6 Volumes (and updates) of the Manual.
- 1-year access to the c4 LEARN digital learning platform.
- 24 hours of live online sessions.
- 1-year access to the c4 Lab (Analyst Edition) valued at $ 1,428
- Live Polygon blockchain tokens for practical learning exercises.
- Interactive quizzes that teach, not just test.
- Operational checklists and decision-making frameworks.
- Authentic court records from real cases.
- Professional Certification

For details and to join, visit:
https://c4academy.com/cryptocurrency-crime-analyst.php

Cryptocurrency Crime Investigator

Build core blockchain tracing and wallet forensics skills to investigate cryptocurrency crime with confidence.

Who is a Cryptocurrency Crime Investigator?

A c4 certified Cryptocurrency Crime Investigator (CCI) is a professional trained to investigate cryptocurrency-related crime — from identifying a suspicious wallet to tracing illicit funds across blockchains and building a case that holds up under scrutiny.

Think of a CCI as someone who knows not just that a transaction is suspicious, but why — and can prove it.

The CCI certification covers three skill areas, built directly from three volumes of the Cryptocurrency Investigation & Forensics Manual:

3 Skills of a CCI

1. **Cryptocurrency Wallet Investigation and Forensics —** You learn to identify and examine wallets, extract ownership leads, and build an investigative picture from addresses, keys, and transaction histories.

2. **Technical Foundations for Digital Investigations —** You understand how blockchains actually work under the hood. So you are never misled by technical complexity — and you can explain what you found to anyone in the room.

3. **Blockchain and Cryptocurrency Investigation —** You follow the money. Across wallets, across exchanges, across the layered obfuscation techniques that criminals use to cover their tracks.

Simply put, a CCI knows how to find the evidence, understand it, and present it with confidence.

Regular Fees

- Fees (India): INR 25,000 + GST
- Fees (International): US$ 299

Early bird discounts, group discounts, and government pricing available.

Everything Included

- 1-year access to Volume 1: Cryptocurrency Wallet Investigation Manual.
- 1-year access to Volume 2: Technical Foundations for Digital Investigations.
- 1-year access to Volume 3: Blockchain & Cryptocurrency Investigation Manual.
- 1-year access to the c4 LEARN digital learning platform.
- Live expert-led online sessions.
- 1-year access to the c4 Lab (Investigator Edition) valued at US$ 468
- Live Polygon blockchain tokens for practical learning exercises.
- Interactive quizzes that teach, not just test.
- Operational checklists and decision-making frameworks.
- Authentic court records from real cases.
- Professional Certification: c4 Certified Cryptocurrency Crime Investigator (CCI).

Meet your Teachers

Rohas Nagpal

Rohas Nagpal is an author, lawyer, and investigator with over 25 years of experience. He has worked across 18 countries on complex cases involving digital forensics, cyber terrorism, financial crime, and corporate liability.

He co-founded Asian School of Cyber Laws in 1999 and has assisted the Government of India in drafting rules under the Information Technology Act.

He authored the Cryptocurrency Investigation & Forensics Manual and the Cyber Crime Investigation Manual, described by The Times of India as the "Bible for cybercrime investigators", and wrote India's first legal commentary on the Information Technology Act.

Rohas first encountered Bitcoin in 2011 during a narcotics investigation, an experience that led to a long-term focus on blockchain, cryptocurrency crime, and financial infrastructure.

He later co-founded BankChain, a blockchain consortium of 37 banks, designed a Layer-1 protocol for regulated finance, and served as a consultant to the Reserve Bank Innovation Hub on NFTs & CBDCs.

He also leads the team developing c4 Lab and c4 Field.

Santosh Khadsare

Santosh Khadsare is an Army veteran, TEDx speaker, and former Scientist E at CERT-In, Ministry of Electronics and IT, Government of India, with over 25 years of experience in digital forensics and incident response.

He has led digital forensics lab operations at CERT-In, handled live cyber incidents, and driven investigator capacity-building for government and law enforcement teams.

His operational focus includes field-to-lab workflows, courtroom-oriented evidence handling, and practical mentoring for investigators working on national-level cyber investigations.

Shinam Arora

Shinam Arora is a computer science engineer with 15+ years of experience in blockchain systems and digital evidence analysis. She is co-founder of BankChain (a consortium of 37 banks with IBM, Microsoft, and Intel), and co-founder of HyFi Blockchain and Sara AI.

She was the co-founder and CEO of Primechain Technologies, where she led teams building blockchain and cyber platforms and worked on applied blockchain use-cases for regulated sectors.

Her work at c4 ensures that investigation training and tooling stay technically accurate to real blockchain behavior, including edge cases investigators face in live cases.

c4 Lab

c4 Lab is a browser-based Cryptocurrency Investigation, Blockchain Forensics, and DeFi Monitoring platform.

c4 Seed — BIP-39 mnemonic analysis pipeline

- Seed Forensics — conceptual/workflow overview for treating mnemonics as forensic evidence
- Seed Investigator — derives addresses from a full phrase and checks on-chain activity across chains to triage relevance fast
- Seed Recovery — reconstructs partial phrases with missing words, validates checksum, and ranks candidates (training + forensic recovery)
- Seed Creator — generates real BIP-39 mnemonics and derives keys/addresses across derivation paths, primarily for training and controlled testing

c4 Wallet — wallet-level analysis

- Wallet Profiler — fast EVM + non-EVM balance/activity snapshot
- Wallet File Analyzer — uploads and inspects wallet files (format detection, metadata extraction, optional key decryption)
- MetaMask Analyzer — parses MetaMask State Logs JSON into a forensic account/transaction summary
- EVM TX Broadcaster — builds, signs, and broadcasts EVM transfers (native + ERC-20)
- UTXO TX Broadcaster — builds/signs/broadcasts legacy P2PKH transactions or broadcasts raw hex

c4 Blockchain — on-chain intelligence

- Transaction Graph — interactive EVM address flow visualization showing inbound/outbound counterparties
- TX Receipt — printable investigation receipt for EVM transactions
- Verbose TX Decoder — decoded input data, event logs, and internal transactions (via Moralis)
- Internal Transfer Analyzer — surfaces internal call transfers often missed in basic transfer lists
- Exchange Address / Ransomware Address — c4 local intelligence databases for flagged addresses
- CryptoScamDB / Address Labels — scam and label enrichment lookups
- Multi-Chain USDT Tracker — USDT transfer tracking across chains

c4 Coins — chain-specific lookups

Bitcoin, Bitcoin Cash, Litecoin, Mempool Monitor, Monero validator, Tron Wallet Profiler, TRC20 Transfer Tracker

c4 DeFi — market and protocol intelligence
DeFi protocol data, TVL by chain, yield pools, stablecoin tracking, de-peg monitor, crypto market overview

c4 Tokens / Contract — token and smart contract analysis
- Token Metadata (symbol or contract address)
- Contract Analyzer + BSC Contract Inspector

c4 Checklists — structured investigative workflows
Ransomware, Rug Pull, Exchange Hack, Wallet Compromise, Romance Scam/Pig Butchering, Money Laundering, NFT Fraud, Darknet Market

c4 Utilities — general investigator toolkit
Encoding/decoding, hashing, datetime tools, regex tester, diff viewer, pattern extractor, CSV viewer, crypto unit calculator, random generators, wallet address generator, and more

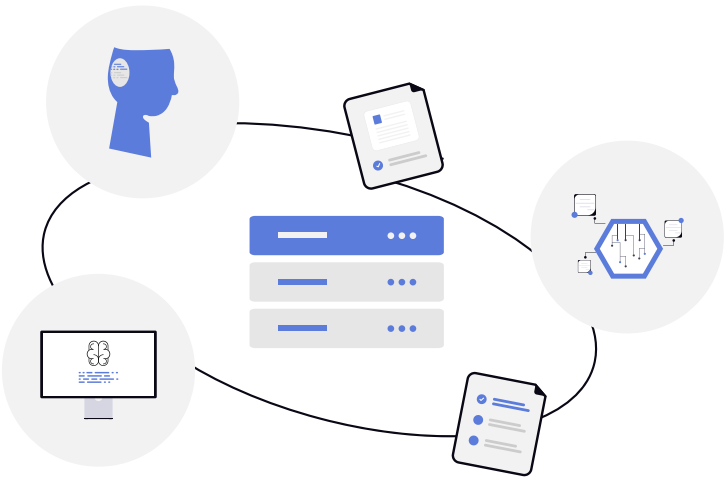
c4 Cyber — OSINT and digital forensics
WHOIS, DNS, IP geolocation, email investigation, username search, domain history, SSL certs, log analyzer, Shodan/Censys, EXIF viewer, OCR, QR decoder, steganography scanner, file hashing, database browser, artifact search

c4 Cryptanalysis — encryption and password tools
AES, 3DES, RC4, ROT, XOR, RSA, PGP, hash tools, password analysis/generation

c4 Field (mobile/endpoint deployment)
Import Manager, Screenshot Capture, Clipboard Grabber, Process Lister, Browser Sessions, Wallet Scanner

Login: https://tools.c4academy.com/login

Pricing: https://tools.c4academy.com/pricing



c4 Field

c4 Field is a USB-deployable forensic acquisition platform built for time-sensitive operations. It captures volatile evidence from live systems before suspects can delete, encrypt, or alter data.

Collectively, c4 Field is designed around one principle: digital evidence that exists right now may not exist in ten minutes. Every tool in the suite is optimised for speed, minimal system footprint, and capturing things that a standard disk image would miss entirely.

No installation. No footprint. You boot it from USB, and the tools run directly on the live system.

Here is what each tool does:

Screenshot Capture grabs the current screen state the moment you arrive. What was open, what was visible, what the suspect was doing — frozen in time before anyone can close a window.

Clipboard Grabber pulls whatever is currently sitting in the clipboard. This sounds minor until you find a seed phrase, a wallet address, or a password that the suspect just copied and hasn't pasted yet.

Process Lister shows every process running on the machine at the moment of acquisition. Encryption tools, VPNs, Tor, coin mixers, wallet software — if it's running, it shows up here. This is how you prove a suspect was actively using a tool, not just that it was installed.

Browser Sessions extracts active browser tabs, session cookies, and browsing history from live browser processes. You can see exactly what sites were open, what accounts were logged in, and what the suspect was looking at in the last few minutes.

Wallet Scanner searches the live filesystem for wallet files, private key files, seed phrase documents, and exchange-related data. It looks in the usual places — AppData, browser profiles, Desktop, Downloads — and flags anything that looks like a crypto artefact.

Network Monitor captures active network connections at the moment of acquisition. Open connections to exchanges, mixers, remote servers, or VPN endpoints. This is the digital equivalent of catching someone mid-call.

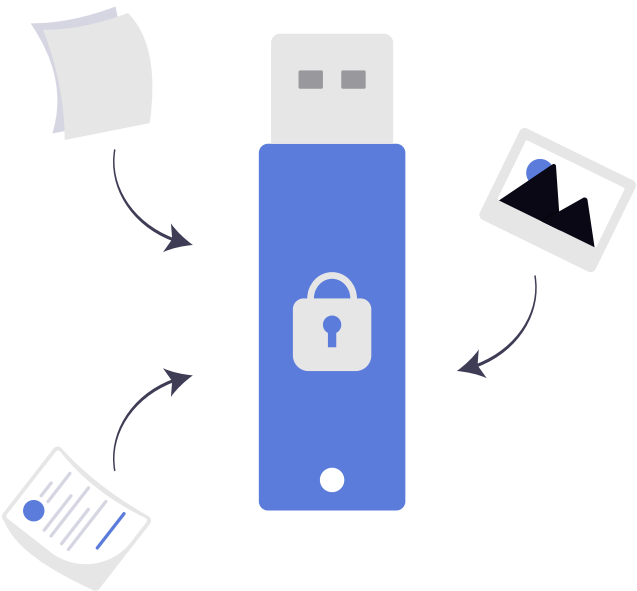
File Finder searches for files matching patterns you specify — by extension, by filename, by content. Looking for `.wallet` files, PDFs with "seed" in the name, or spreadsheets in an unusual location? This finds them without a full disk image.

Memory Strings extracts printable strings from live RAM. Passwords, addresses, URLs, chat messages, seed phrases — anything that was in active memory at the time of acquisition. RAM is volatile. The moment the machine shuts down, this evidence is gone forever.

Memory Dump captures a full image of live RAM for deeper offline analysis. This is the raw evidence. A forensic examiner can load it into tools like Volatility later to reconstruct processes, decrypt in-memory wallets, and recover artefacts that were never written to disk.

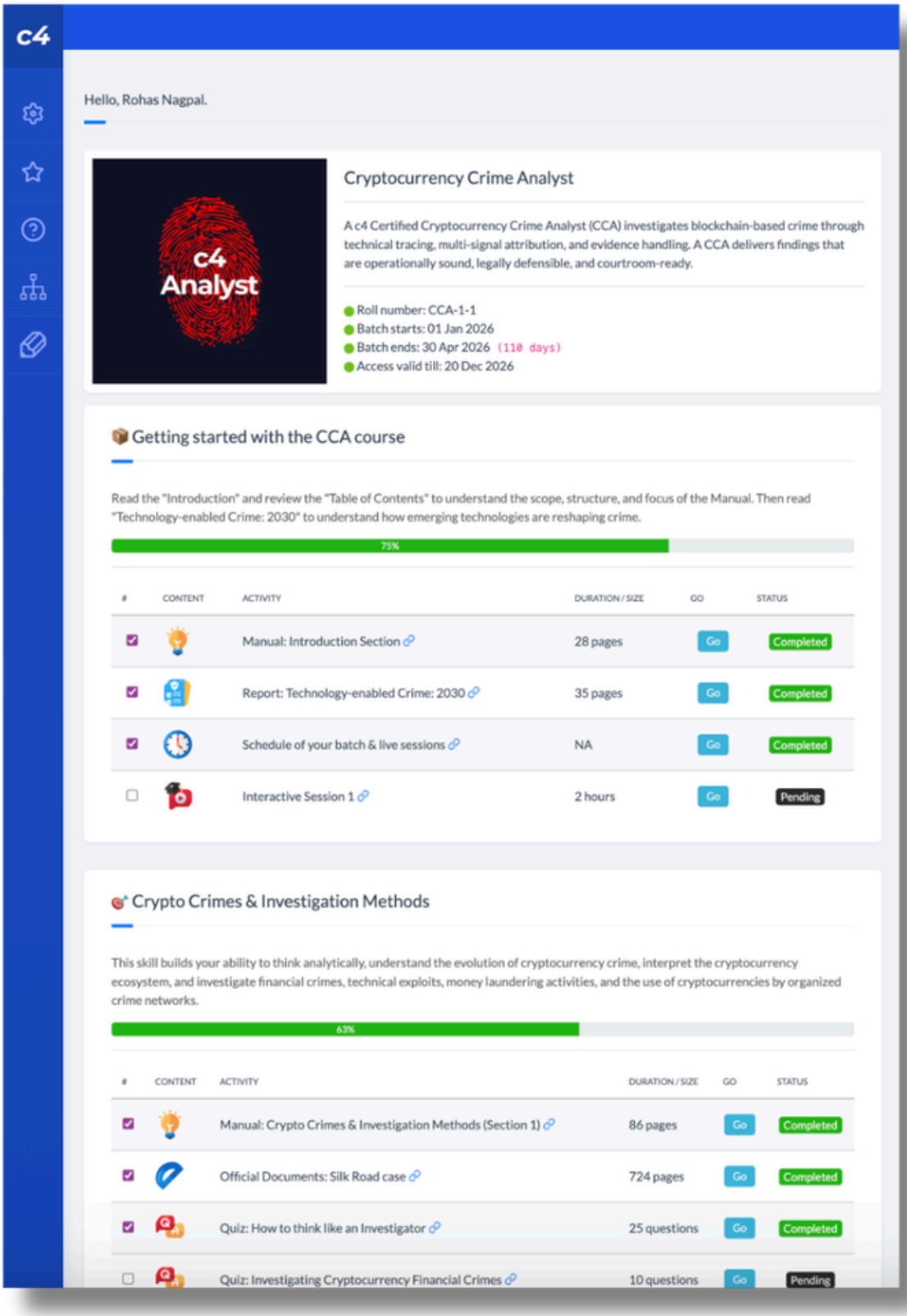
Android Acquisition connects to an unlocked Android device over ADB and extracts installed apps, SMS, call logs, contacts, and accessible app data. Crypto apps, exchange apps, authenticator apps — if the phone is unlocked and connected, you can pull evidence from it right there.

Evidence Timeline takes all acquired artefacts and assembles them into a single chronological timeline — file timestamps, browser activity, process start times, network connections. Instead of a pile of raw data, you get a story: what happened, in what order, on what device.



c4 LEARN

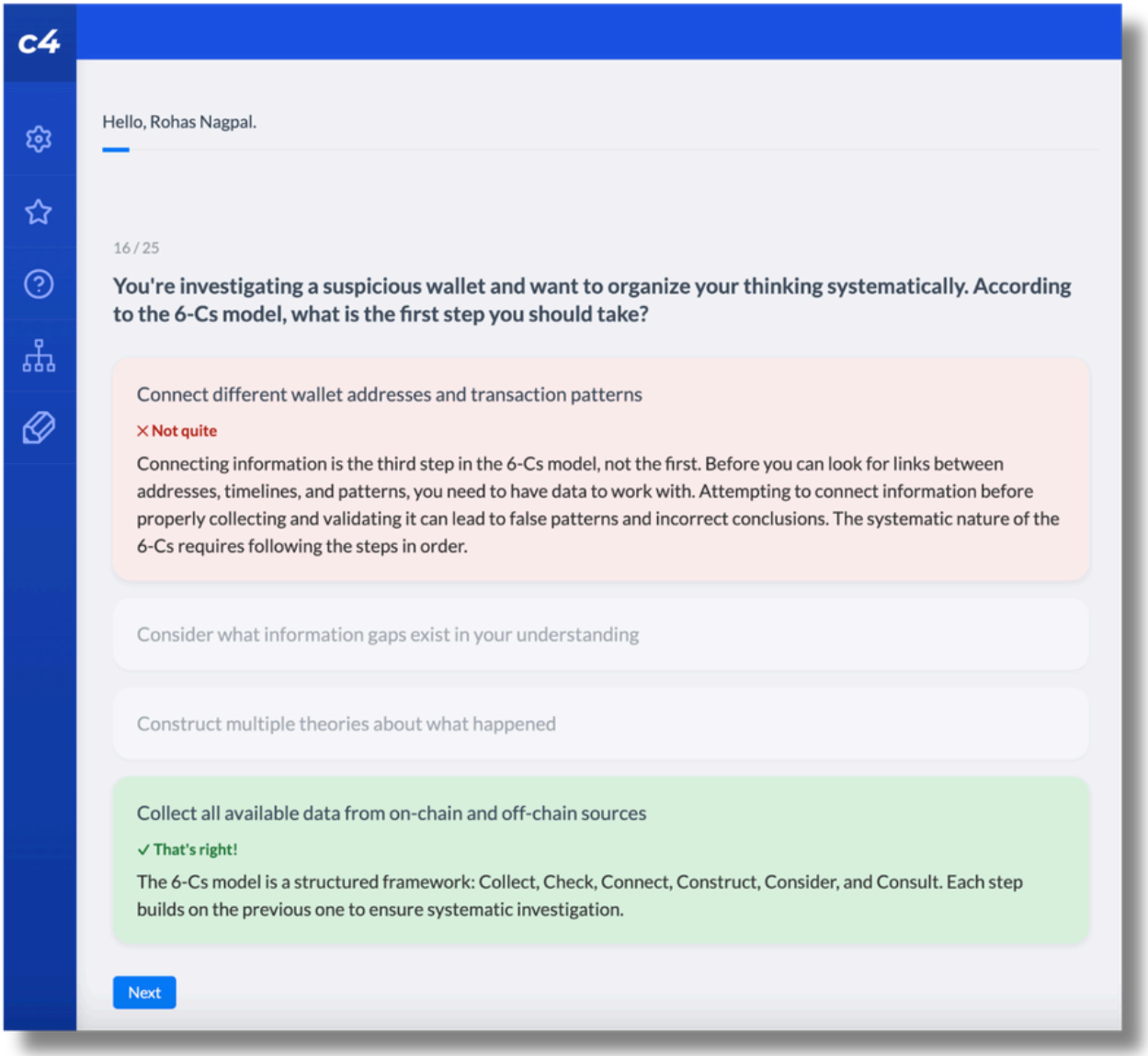
The c4 LEARN digital platform powers the CCA course with Interactive Quizzes, Deep-dive Videos. Court Records, and Official Documents.

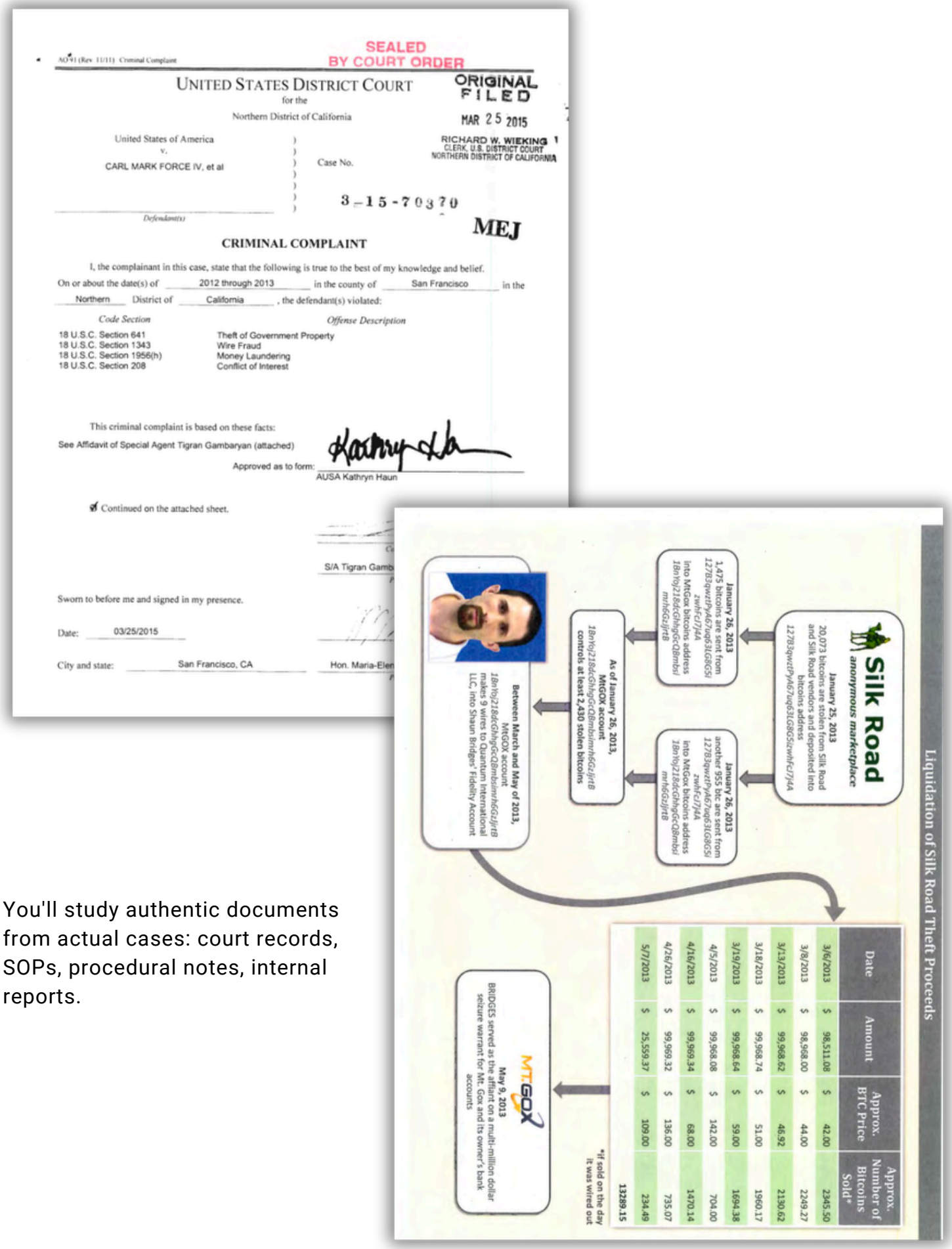


Every c4 Interactive Quiz is designed to teach, not just test.

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

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