Dark Web and Cryptocurrencies in Criminal Investigations Training Course

Professional Development Training Course Outline

Category	Criminology	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s evolving digital ecosystem, the dark web and cryptocurrencies have emerged as both technological advancements and significant challenges for law enforcement, cybercrime investigators, and financial intelligence units. As cybercriminals exploit anonymity tools and decentralized finance platforms to engage in illicit trade, money laundering, identity theft, and terrorism financing, it has become imperative for criminal justice professionals to acquire specialized skills in dark web investigations and cryptocurrency forensics. Training Course on Dark Web & Cryptocurrencies in Criminal Investigations provides actionable insights and hands-on training to enhance digital evidence gathering and improve cyber-enabled crime detection capabilities.

With a strong emphasis on blockchain analysis, crypto-wallet tracking, and anonymity network infiltration, this course empowers investigators with techniques to trace illegal financial flows, identify darknet marketplaces, and decode encryption patterns used by sophisticated cybercriminals. Participants will gain in-depth understanding of the darknet landscape, virtual assets, privacy coins, and tools like Tor, I2P, mixers, and tumblers—critical to developing intelligence-led approaches for digital crime prevention and financial crime investigation.

Programme Curriculum

Dark Web and Cryptocurrencies in Criminal Investigations Training Course

Introduction

In today’s evolving digital ecosystem, the dark web and cryptocurrencies have emerged as both technological advancements and significant challenges for law enforcement, cybercrime investigators, and financial intelligence units. As cybercriminals exploit anonymity tools and decentralized finance platforms to engage in illicit trade, money laundering, identity theft, and terrorism financing, it has become imperative for criminal justice professionals to acquire specialized skills in dark web investigations and cryptocurrency forensics. Dark Web and Cryptocurrencies in Criminal Investigations Training Course provides actionable insights and hands-on training to enhance digital evidence gathering and improve

cyber-enabled crime detection capabilities.

With a strong emphasis on blockchain analysis, crypto-wallet tracking, and anonymity network infiltration, this course empowers investigators with techniques to trace illegal financial flows, identify darknet marketplaces, and decode encryption patterns used by sophisticated cybercriminals. Participants will gain in-depth understanding of the darknet landscape, virtual assets, privacy coins, and tools like Tor, I2P, mixers, and tumblers—critical to developing intelligence-led approaches for digital crime prevention and financial crime investigation.

Course Objectives

1. Understand the structure and functionality of the dark web and Tor network.
2. Identify common cryptocurrency types used in illicit transactions.
3. Apply blockchain tracing techniques to investigate suspicious crypto movements.
4. Conduct open-source intelligence (OSINT) on darknet forums and marketplaces.
5. Examine techniques for de-anonymizing transactions and linking wallet addresses.
6. Evaluate methods used in crypto laundering and chain-hopping.
7. Use digital forensics tools for crypto and dark web investigations.
8. Assess the role of privacy coins (e.g., Monero, Zcash) in criminal activity.
9. Analyze international regulations on virtual asset service providers (VASPs).
10. Investigate use of decentralized finance (DeFi) in cyber-enabled crime.
11. Document evidence from dark web sources for court admissibility.
12. Implement multi-agency strategies for cross-border crypto investigations.
13. Identify red flags and typologies of terrorism financing via crypto.

Target Audiences

1. Law Enforcement Officers
2. Cybercrime Investigators
3. Financial Intelligence Analysts
4. Compliance & Risk Officers
5. Customs & Border Protection Agents
6. Prosecutors & Legal Experts
7. Intelligence Officers
8. Blockchain Forensic Analysts

Course Duration: 10 days

Course Modules

Module 1: Introduction to the Dark Web and Deep Web

- Understanding the surface web, deep web, and dark web
- Key access methods: Tor, I2P, and anonymity protocols
- Darknet marketplaces and communication patterns
- Darknet vendor profiling
- Real-world dark web statistics
- **Case Study**: Silk Road Takedown and Law Enforcement Strategy

Module 2: Overview of Cryptocurrencies in Criminal Use

- Bitcoin, Ethereum, and privacy coins in crime
- Wallets, exchanges, and P2P networks
- Cryptocurrency typologies in cybercrime
- Identifying illegal crypto patterns
- Global crypto adoption and misuse

- **Case Study**: Use of Monero in Ransomware Payments

Module 3: Blockchain Technology & Forensics

- Basics of blockchain structure
- Public vs. private ledgers
- Chain analysis and crypto flow tracking
- Smart contract forensics
- Forensic platforms: Chainalysis, CipherTrace, Elliptic
- **Case Study**: Tracing a $10M Crypto Theft via Ethereum

Module 4: OSINT for Dark Web Investigations

- Scraping dark web forums
- Analyzing vendor reviews and digital signatures
- Monitoring Telegram, Discord, and dark web mirrors
- Building threat actor profiles
- Secure methods for dark web infiltration
- **Case Study**: Infiltrating an Illicit Darknet Pharmacy

Module 5: Crypto Wallets, Mixers, and Tumblers

- Types of wallets: custodial, non-custodial, hardware
- Functionality of mixers and coinjoin tools
- Chain-hopping and obfuscation tactics
- Identifying wallet clustering
- Wallet attribution techniques
- **Case Study**: Uncovering a Crypto Mixing Operation

Module 6: Digital Evidence and Legal Considerations

- Evidence collection protocols
- Ensuring chain of custody in digital evidence
- Metadata extraction from dark web tools
- Reporting formats for courts
- Legal frameworks for crypto seizure
- **Case Study**: Crypto Evidence Admitted in Court

Module 7: Ransomware, Extortion & Crypto Payments

- Anatomy of a ransomware attack
- Identifying ransom payment addresses
- Coordinating with crypto exchanges
- Recovering stolen funds
- Tracking funds through privacy coins
- **Case Study**: Colonial Pipeline Ransom Payment Analysis

Module 8: Crypto Laundering Techniques

- Typologies of laundering in virtual currencies
- Layering through NFTs and DeFi
- Use of shell companies and fake ICOs
- Red flag indicators in exchanges
- Cross-chain laundering strategies
- **Case Study**: DeFi Platform Used in Drug Trafficking Scheme

Module 9: Privacy Coins & Anonymity Challenges

- Comparing Monero, Dash, and Zcash
- Obfuscation techniques in privacy coins
- Identifying transactions with partial traceability
- Use of zero-knowledge proofs
- Surveillance countermeasures
- **Case Study**: FBI Investigation Involving Zcash Payments

Module 10: Crypto Exchanges and VASPs

- KYC/AML compliance requirements
- Exchange behavior analysis
- Investigating decentralized exchanges (DEXs)
- Red flags in trading behavior
- Coordinating subpoenas and requests
- **Case Study**: Binance Compliance Case and VASP Cooperation

Module 11: Investigative Tools and Software

- Top forensic platforms overview
- Features of crypto transaction graphing tools
- Evidence reporting templates
- Real-time monitoring systems
- Secure data extraction methods
- **Case Study**: Crypto Analysis with Chainalysis Reactor

Module 12: International Regulations and Frameworks

- FATF guidelines on VASPs
- Differences in crypto laws across countries
- Collaboration through INTERPOL, EUROPOL, UNODC
- Understanding travel rule enforcement
- Legal gaps and challenges
- **Case Study**: Cross-Border Crypto Case in Europe and Asia

Module 13: Terrorist Financing and Crypto

- Indicators of extremist funding
- Analyzing wallets linked to known terror groups
- Identifying micro-donations and covert fundraising
- Monitoring propaganda sites with crypto donations
- Strategic policy implications
- **Case Study**: ISIS-Linked Crypto Wallets Investigation

Module 14: Crypto Asset Recovery & Seizure

- Techniques for seizing private keys
- Custody and secure storage of digital assets
- Legal documentation required
- Challenges in asset liquidation
- Post-seizure fund tracing
- **Case Study**: DOJ Seizure of $1 Billion in Bitcoin

Module 15: Future Trends and Cybercrime Evolution

- Rise of AI in cybercrime
- Web3 and Metaverse crime potential

- Impact of quantum computing on blockchain
- Predictive analytics in crypto forensics
- Law enforcement adaptation strategies
- **Case Study**: Predicting Crime Patterns in Metaverse Platforms

Training Methodology

- Instructor-led interactive lectures
- Hands-on exercises with forensic tools
- Dark web lab simulations in secure environments
- Group discussions and real-life scenario debriefs
- Case-based learning and expert guest speakers
- Access to downloadable forensic datasets and templates

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com