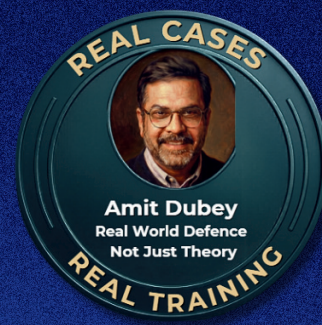




MODULE 12: DARK WEB & CRYPTOCURRENCY INVESTIGATION AND FORENSICS



Module Objective:

Dark web intelligence • Evidence preservation • Blockchain tracing • Identity correlation • Court-ready reporting

Curriculum

SEGMENT 12.1 – Surface Web vs Deep Web vs Dark Web

Topics:

- Web layer classification
- TOR network architecture
- I2P and Freenet overview
- Hidden services (.onion)
- Legal and ethical boundaries

SEGMENT 12.2 – Dark Web Access & Operational Security (OPSEC)

Topics:

- Secure VM setup
- TOR browser configuration
- VPN chaining
- DNS & WebRTC leak prevention
- Identity compartmentalization
- Digital fingerprinting risks

SEGMENT 12.3 – Dark Web Marketplace Investigation

Topics:

- Marketplace structures
- Vendor reputation systems
- Escrow mechanisms
- Product categorization
- Price pattern analysis
- Evidence Types:
- Listing screenshots
- Vendor profiles
- PGP keys
- Transaction instructions
- Delivery methods

SEGMENT 12.4 – Dark Web Crime Categories

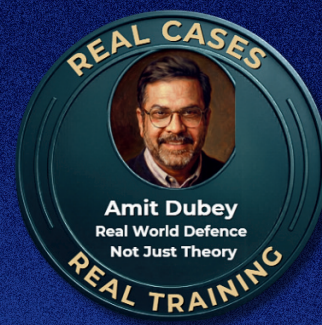
Topics:

- Drugs & narcotics
- Weapons
- Fake documents
- Data dumps
- Hacking services
- Malware rentals
- Child exploitation material (legal handling only)





MODULE 12: DARK WEB & CRYPTOCURRENCY INVESTIGATION AND FORENSICS



SEGMENT 12.5 – Dark Web OSINT & HUMINT

Topics

- Forum infiltration
- Language pattern profiling
- Username reuse tracking
- Cross-platform identity linkage
- Social engineering indicators

SEGMENT 12.6 – Evidence Preservation from Dark Web

Topics

- Screenshot authenticity
- HTML source capture
- Timestamp validation
- Hash verification
- Metadata preservation
- Chain of custody

SEGMENT 12.7 – Cryptocurrency Fundamentals

Topics

- Blockchain basics
- Wallet types
- Public vs private keys
- Transactions & blocks
- Mining & validators

SEGMENT 12.8 – Cryptocurrency Crime Use Cases

Topics

- Crime Type- Crypto Role
- Ransomware- Payment
- Drug trade- Settlement
- Terror funding- Transfer
- Scams- Fraud
- Money laundering- Layering

SEGMENT 12.9 – Blockchain Analysis Techniques

Topics

- Transaction tracing
- Cluster analysis
- Change address detection
- Mixer identification
- Exchange tagging
- Wallet behavior profiling

SEGMENT 12.10 – Privacy Coins & Challenges

Coins:

- Monero
- Zcash
- Dash

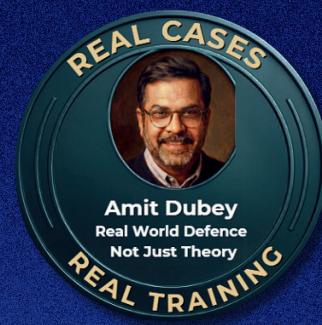
Challenges:

- Ring signatures
- Stealth addresses
- Zero-knowledge proofs





MODULE 12: DARK WEB & CRYPTOCURRENCY INVESTIGATION AND FORENSICS



SEGMENT12.11 – De-Anonymization Strategies

Techniques:

- Exchange KYC correlation
- IP leak correlation
- Behavioral spending patterns
- Service reuse detection
- Timing correlation
- SEGMENT12.12 – Dark Web + Crypto Correlation

Correlation Points:

- Wallet addresses in listings
- Escrow wallet tracking
- Vendor wallet reuse
- Feedback timeline mapping

SEGMENT12.13 – Evidence Identification

Crypto Evidence:

- Wallet addresses
- Transaction hashes
- Block numbers
- Amount patterns
- Exchange deposits

Dark Web Evidence:

- Vendor identity
- Listings
- PGP keys
- Communication logs

SEGMENT12.14 – Legal & Court Presentation

- Blockchain evidence admissibility
- Expert testimony
- Report formatting
- Visualization charts
- Jurisdiction challenges
- SEGMENT12.15 – Practical Case Study

Scenario:

- Dark web drug vendor
- Bitcoin wallet tracing
- Exchange correlation
- Identity identification
- Final forensic report

