

CRYPTOCURRENCY CRIME SCENE: FIRST RESPONDER MANUAL



ROHAS NAGPAL

Table of Contents

SECTION 1: FOUNDATION & FRAMEWORK

1.1 Introduction.....	16
1.1.1 Purpose and Scope	
1.1.2 How to Use This Manual	
1.1.3 When to Deviate from Procedures	
1.2 First Responder Roles.....	18
1.2.1 Team Leader	
1.2.2 Evidence Collector	
1.2.3 Documentation Officer	
1.2.4 Scene Security	
1.3 Legal Authority Basics.....	20
1.3.1 Search and Seizure Authority	
1.3.2 Asset Transfer Authority	
1.3.3 Emergency Action Authorization	
1.4 Training Requirements.....	22
1.4.1 Minimum Training Standards	
1.4.2 Practical Skills Assessment	
1.4.3 Continuing Education	

SECTION 2: PRE-INCIDENT PREPARATION

2.1 Agency Seizure Wallet Infrastructure.....	24
2.1.1 Multi-Signature Wallet Setup	
2.1.2 Supported Blockchain Networks	
2.1.3 Key Management Protocols	
2.1.4 Wallet Address Registry	
2.1.5 Emergency Access Procedures	
2.2 Equipment Checklist.....	26
2.2.1 Required Equipment	
2.2.2 Faraday Bags and Signal Blockers	
2.2.3 Photography Equipment	
2.2.4 Evidence Collection Materials	
2.2.5 Battery Packs and Power Solutions	
2.2.6 Equipment Testing	

2.3 Legal Documentation and Forms.....	30
2.3.1 Search Authorization	
2.3.2 Asset Seizure Forms	
2.3.3 Chain of Custody Forms	
2.3.4 Asset Transfer Authorization	

2.4 Pre-Operation Planning.....	33
2.4.1 Intelligence Review	
2.4.2 Target Assessment	
2.4.3 Known Wallet Addresses	
2.4.4 Drain Risk Pre-Assessment	
2.4.5 Team Briefing	

SECTION 3: INITIAL RESPONSE & SCENE OPERATIONS

3.1 Scene Arrival and Entry.....	38
3.1.1 Entry Strategy	
3.1.2 Scene Security	
3.1.3 Suspect/Witness Control	

3.2 Critical First 60 Seconds.....	41
3.2.1 Immediate Threat Assessment	
3.2.2 Visible Device Identification	
3.2.3 Screen State Preservation	
3.2.4 Suspect Separation from Devices	

3.3 Five-Minute Scene Assessment.....	44
3.3.1 Scene Survey	
3.3.2 Device Inventory (Preliminary)	
3.3.3 Environmental Factors (Power, Network)	
3.3.4 Complexity Evaluation	
3.3.5 When to Call for Backup/Specialists	

3.4 Crypto Crime Scene Indicators.....	48
3.4.1 Hardware Wallet Recognition	
3.4.2 Mining Equipment	
3.4.3 Trading Workstations	
3.4.4 Paper Wallets and Seed Phrases	
3.4.5 Common Hiding Locations	

SECTION 4: DEVICE IDENTIFICATION & CATEGORIZATION

4.1 Hardware Wallets.....	52
4.1.1 Ledger Devices	
4.1.2 Trezor Devices	
4.1.3 Other Hardware Wallets	
4.1.4 PIN Status and Attempts	
4.1.5 Handling Procedures	
4.2 Software Wallets.....	57
4.2.1 Desktop Applications	
4.2.2 Mobile Apps	
4.2.3 Browser Extensions	
4.2.4 Web-Based Wallets	
4.3 Paper Wallets and Physical Storage.....	61
4.3.1 Paper Wallet Formats	
4.3.2 QR Codes	
4.3.3 Seed Phrases (12/24 word)	
4.3.4 Metal Backup Plates	
4.3.5 Collection Procedures	
4.4 Exchange Access Devices.....	66
4.4.1 Active Sessions	
4.4.2 Saved Credentials	
4.4.3 Two-Factor Authentication	
4.4.4 Email Access	
4.5 Mining Equipment.....	70
4.5.1 ASIC Miners	
4.5.2 GPU Rigs	
4.5.3 Pool Configuration	
4.5.4 Associated Wallets	

SECTION 5: CRITICAL "DO NOT" PROTOCOLS

5.1 Power State Management.....	74
5.1.1 Never Disconnect Power Without Assessment	
5.1.2 Timeout Prevention	
5.1.3 Battery Backup Procedures	
5.1.4 Controlled Shutdown Decision	

5.2 Network Connectivity.....	76
5.2.1 Never Auto-Disconnect Network	
5.2.2 Network State Assessment	
5.2.3 Isolation vs. Monitoring	
5.2.4 Faraday Bag Timing	
5.3 Device Interaction.....	78
5.3.1 Minimize Interaction	
5.3.2 Accidental Input Prevention	
5.3.3 When Interaction Is Necessary	
5.4 Password and Seed Phrase Handling.....	80
5.4.1 Never Discard Written Materials	
5.4.2 Search Methodology	
5.4.3 Secure Transport	
5.5 Screen State Documentation.....	82
5.5.1 Photograph Before Any Interaction	
5.5.2 Multi-Angle Photos	
5.5.3 Video Recording	
5.5.4 Timestamp Synchronization	
5.6 Common Mistakes to Avoid.....	84

SECTION 6: IMMEDIATE ASSET PRESERVATION

6.1 Drain Risk Assessment.....	86
6.1.1 Risk Indicators	
6.1.2 Hot Wallet Identification	
6.1.3 Remote Access Threats	
6.1.4 Time Sensitivity	
6.1.5 Asset Value Thresholds	
6.2 Transfer vs. Isolation Decision.....	88
6.2.1 Decision Tree	
6.2.2 When to Transfer Immediately	
6.2.3 When Isolation Is Sufficient	
6.2.4 When to Call Specialists	
6.3 Legal Authorization Verification.....	90
6.3.1 Search Authority Confirmation	
6.3.2 Asset Transfer Authority	
6.3.3 Supervisor Approval	
6.3.4 Documentation Requirements	

6.4 Wallet Discovery and Access.....	92
6.4.1 Unlocked Device Procedures	
6.4.2 Active Wallet Sessions	
6.4.3 Hardware Wallet Connection	
6.4.4 Seed Phrase Recovery	
6.5 Asset Balance Documentation.....	94
6.5.1 Screenshot Requirements	
6.5.2 Block Explorer Verification	
6.5.3 Multi-Asset Inventory	
6.5.4 Witness Verification	
6.6 Emergency Asset Transfer Execution.....	95
6.6.1 Pre-Transfer Checklist	
6.6.2 Agency Wallet Confirmation	
6.6.3 Multi-Witness Requirement	
6.6.4 Transaction Construction	
6.6.5 Gas Fee Considerations	
6.6.6 Transaction Broadcast	
6.6.7 Blockchain Confirmation	
6.6.8 Transaction Hash Recording	
6.7 Post-Transfer Documentation.....	97
6.7.1 Before/After Screenshots	
6.7.2 Block Explorer Confirmation	
6.7.3 Witness Signatures	
6.7.4 Chain of Custody Updates	
6.8 Locked Device Scenarios.....	98
6.8.1 Biometric Access Opportunities	
6.8.2 Voluntary Disclosure	
6.8.3 Device Isolation	
6.8.4 Specialist Escalation	

SECTION 7: EVIDENCE COLLECTION

7.1 Scene Photography and Video.....	100
7.1.1 Overall Scene (360° Coverage)	
7.1.2 Device Location Photos	
7.1.3 Screen Content (Critical)	
7.1.4 Cables and Connections	
7.1.5 Serial Numbers	
7.1.6 Scale References	
7.1.7 Video Walkthrough	

7.2 Physical Evidence Collection.....	102
7.2.1 Powered Device Handling	
7.2.2 Powered-Off Device Handling	
7.2.3 Hardware Wallet Collection	
7.2.4 Cables and Accessories	
7.2.5 Packaging and Labeling	
7.2.6 Anti-Static Bags	
7.3 Digital Evidence Capture.....	104
7.3.1 Screen Recording	
7.3.2 Network State Documentation	
7.3.3 Open Applications	
7.3.4 Browser History (If Accessible)	
7.4 Seed Phrase and Password Search.....	105
7.4.1 Systematic Search Protocol	
7.4.2 Written Notes and Notebooks	
7.4.3 Safes and Secure Storage	
7.4.4 Digital Files	
7.4.5 Email and Cloud Storage	
7.4.6 Password Managers	
7.4.7 USB Drives	
7.4.8 Physical Hiding Locations	
7.4.9 Metal Backup Plates	
7.5 Exchange Account Documentation.....	107
7.5.1 Platform Identification	
7.5.2 Account Credentials	
7.5.3 Two-Factor Authentication	
7.5.4 Transaction History Screenshots	
7.5.5 Email Confirmations	
7.6 Associated Documentation.....	109
7.6.1 Financial Records	
7.6.2 Purchase Receipts	
7.6.3 Mining Pool Info	
7.6.4 Communication Records	
7.6.5 Handwritten Notes	

SECTION 8: CHAIN OF CUSTODY

8.1 Initial Custody Documentation.....	110
8.1.1 Form Completion	
8.1.2 Date, Time, Location	
8.1.3 Item Description	
8.1.4 Serial Numbers and Identifiers	
8.1.5 Condition Assessment	
8.1.6 Witness Signatures	
8.2 Crypto-Specific Custody Fields.....	112
8.2.1 Wallet Addresses	
8.2.2 Balance at Seizure	
8.2.3 Asset Types and Quantities	
8.2.4 Transfer Transaction Hashes	
8.2.5 Agency Receiving Wallets	
8.3 Transfer and Handoff.....	114
8.3.1 Transfer Authorization	
8.3.2 Physical Inspection	
8.3.3 Signature Requirements	
8.3.4 Seal Integrity	
8.4 Storage and Access.....	115
8.4.1 Secure Storage Requirements	
8.4.2 Access Logging	
8.4.3 Storage Location Documentation	

SECTION 9: TRANSPORT AND STORAGE

9.1 Transport Protocols.....	116
9.1.1 Powered Device Transport	
9.1.2 Vehicle Preparation	
9.1.3 Temperature Controls	
9.1.4 Vibration Protection	
9.1.5 Transport Security	
9.2 Storage Facility Standards.....	118
9.2.1 Physical Security	
9.2.2 Climate Control	
9.2.3 Access Control	
9.2.4 Fire/Water Protection	

9.3 Evidence Organization.....	119
9.3.1 Storage Location Assignment	
9.3.2 Case Number Organization	
9.3.3 Retrieval Procedures	

SECTION 10: SPECIAL SCENARIOS

10.1 Exchange-Based Assets.....	120
10.1.1 Centralized Exchange Seizures	
10.1.2 Account Freeze Procedures	
10.1.3 Withdrawal Prevention	
10.2 DeFi Protocols.....	121
10.2.1 DeFi Identification	
10.2.2 Staked Assets	
10.2.3 Time-Locked Assets	
10.2.4 When to Call Specialists	
10.3 NFTs.....	122
10.3.1 NFT Identification	
10.3.2 Marketplace Access	
10.3.3 NFT Transfer Procedures	
10.4 Privacy Coins.....	123
10.4.1 Monero (XMR)	
10.4.2 Zcash (ZEC)	
10.4.3 Mixing Services	
10.4.4 Enhanced Documentation	
10.5 Multi-Signature Wallets.....	124
10.5.1 Multi-Sig Identification	
10.5.2 Co-Signer Location	
10.5.3 Threshold Schemes	
10.6 Mining Operations (Large Scale).....	125
10.6.1 Facility Seizures	
10.6.2 Equipment Inventory	
10.6.3 Pool Operator Scenarios	
10.7 Sophisticated Threat Actors.....	126
10.7.1 Advanced OpSec	
10.7.2 Anti-Forensic Techniques	
10.7.3 Dead Man's Switches	
10.7.4 Remote Wipe Capabilities	

10.8 Active Trading Situations.....	127
10.8.1 Trading Session Interruption	
10.8.2 Trading Bot Shutdown	
10.8.3 Open Position Documentation	

SECTION 11: POST-SEIZURE PROCEDURES

11.1 Immediate Actions.....	128
11.1.1 Scene Clearance	
11.1.2 Evidence Verification	
11.1.3 Preliminary Report	
11.1.4 Supervisor Notification	
11.2 Handoff to Specialists.....	129
11.2.1 Evidence Transfer	
11.2.2 Briefing Requirements	
11.2.3 Contact Information Exchange	
11.3 After-Action Review.....	130
11.3.1 What Went Well	
11.3.2 What Needs Improvement	
11.3.3 Lessons Learned	

APPENDICES

Field Checklists

1. Scene Arrival and Initial Assessment.....	131
2. Powered-on Device Handling.....	133
3. Immediate Asset Transfer Protocol.....	135
4. Hardware Wallet Seizure.....	137
5. Mobile Device Seizure.....	139
6. Computer / Laptop Seizure.....	141
7. Seed Phrase and Password Search.....	143
8. Exchange and Online Account Documentation.....	146
9. Evidence Photography and Documentation.....	149
10. Chain of Custody.....	152
11. Mining Operation Seizure.....	155
12. DeFi/Smart Contract Interaction.....	160
13. Multi-Signature Wallet Handling.....	164

14. Privacy Coin Handling.....	167
15. Transport and Storage.....	171
16. Post-Seizure Immediate Actions.....	175
17. Pre-Operation Preparation.....	179
18. Quality Assurance Review.....	183
 Photo Atlas: Physical Crypto Evidence.....	 188

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 is the co-founder of the Asian School of Cyber Laws, a pioneering institution in cyber law and digital forensics education, and has assisted the Government of India in drafting rules under the Information Technology Act.

He authored the Cryptocurrency Investigation & Forensics Manual 2026 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.

