

COVERT DIGITAL INFRASTRUCTURE INVESTIGATION MANUAL



ROHAS NAGPAL

Table of Contents

A. Investigating Decentralized Domains.....	10
A1. Ethereum Name Service (ENS).....	11
A2. Handshake.....	12
A3. Unstoppable Domains.....	13
A4. Investigative Approaches to Decentralized Domains.....	14
c4 Checklist for Decentralized Domain Investigation.....	17
 B. Investigating Decentralized Hosting and Storage Protocols.....	 19
B1. Arweave.....	20
B2. Filecoin.....	22
B3. IPFS.....	24
B4. Sia.....	27
B5. Storj.....	29
B6. Investigative Approaches to Decentralized Storage Protocols.....	31
c4 Checklist for Decentralized Storage Investigation.....	34
 C. Investigating Emails.....	 35
C1. Ethermail.....	36
C2. Gmail.....	38
C3. Proton Mail.....	41
C4. Tutanota.....	44
C5. Temp email services.....	47
C6. Self-hosted email servers.....	51
 D. Investigating Encrypted & Obfuscated Data.....	 56
D1. Encrypted Containers & Disks.....	57
D2. Encryption & Password Attacks.....	60
D3. Investigator-Safe Handling & Chain of Custody.....	63
D4. Key Management Failures.....	66
D5. Memory & Live-System Analysis.....	69
D6. Metadata & File Artifacts.....	72
D7. Mobile & Cloud Encryption Artifacts.....	76

D8. Steganography & Hidden Data.....	78
D9. Temporary / Disposable Services.....	81
D-10. Investigative Approaches to Encrypted & Obfuscated Data.....	83
c4 Checklist for Encrypted Data Investigation.....	85
E. Investigating Encrypted Messaging Platforms.....	86
E1. Blockscan Chat.....	87
E2. Discord.....	89
E3. Element.....	92
E4. Session.....	95
E5. Signal.....	98
E6. Telegram.....	102
E7. Threema.....	105
E8. WhatsApp.....	108
E-9. Investigative Approaches to Encrypted Messaging Platforms.....	112
c4 Checklist for Encrypted Messaging Investigation.....	115
F. Investigating Parallel Internets.....	116
F1. Freenet (formerly HyphaNet).....	117
F2. GNUnet.....	120
F3. I2P.....	122
F4. Lokinet.....	125
F5. Mix Networks.....	127
F6. Tor.....	129
F7. ZeroNet.....	133
F8. Investigative Approaches to Parallel Internets.....	136
c4 Checklist for Parallel Internet Investigation.....	140
G. Investigating Privacy-Focused Browsers.....	141
G1. Brave Browser.....	142
G2. DuckDuckGo Browser.....	146
G3. LibreWolf.....	149
G4. Mullvad Browser.....	152
G5. Tor Browser.....	155
G6. Investigative Approaches to Privacy-Focused Browsers.....	160
c4 Checklist for Privacy-Focused Browser Investigation.....	164

H. Investigating Privacy-Focused Operating Systems.....	165
H1. CalyxOS.....	166
H2. GrapheneOS.....	169
H3. Kicksecure.....	172
H4. Linux Kodachi.....	175
H5. Qubes OS.....	178
H6. Subgraph OS (Citadel).....	182
H7. Tails.....	184
H8. Whonix.....	187
H9. Investigative Approaches to Privacy Operating Systems.....	191
c4 Checklist for Privacy OS Investigation.....	195
 I. Investigating Proxy & Obfuscation Tools.....	 196
I-1. Lantern.....	197
I-2. Outline.....	199
I-3. Psiphon.....	202
I-4. Shadowsocks.....	204
I-5. Socks5 Proxies.....	207
I-6. SSH Tunneling.....	210
I-7. Surge.....	213
I-8. V2Ray.....	215
I-9. VPN Services.....	218
I-10. WireGuard.....	221
I-11. Investigative Approaches to Proxy & Obfuscation Tools.....	224
c4 Checklist for Proxy & Obfuscation Tool Investigation.....	227

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.

