Scambusters OSINT Investigation Process

Overview
Scambusters is an OSINT-focused initiative that investigates cryptocurrency scams using publicly available information. The goal is to identify scam infrastructure, trace stolen funds, connect related accounts and wallets, and document evidence for awareness and reporting.

1. Initial Lead Collection
Investigations begin with suspicious wallet addresses, phishing websites, fake social media accounts, Telegram or Discord groups, and victim reports. Evidence such as screenshots, transaction hashes, usernames, and URLs is preserved immediately.

2. Blockchain & Wallet Analysis
Investigations focus on tracing stolen cryptocurrency, identifying connected wallets, detecting laundering patterns, and analyzing exchange interactions. Common tools include Etherscan, BscScan, Arkham Intelligence, Breadcrumbs, and blockchain graphing tools.

3. Infrastructure & Domain Analysis
Scam websites are investigated using WHOIS lookups, passive DNS analysis, reverse IP lookups, SSL certificate analysis, and subdomain enumeration. Common indicators include newly created domains, reused hosting infrastructure, and typo-squatted websites.

4. Social Media & Persona Investigation
Scammers often rely on fake online identities across platforms such as X/Twitter, Telegram, Discord, Instagram, LinkedIn, and YouTube. Analysis focuses on stolen profile images, recently created accounts, coordinated posting behavior, username reuse, and fake engagement activity.

5. Intelligence Correlation & Reporting
The final stage combines wallet tracing, infrastructure analysis, and persona investigations into a complete intelligence picture. Reports include scam structure analysis, wallet activity, infrastructure mapping, screenshots, timelines, and investigative findings.

Core Skills Used
- Open-Source Intelligence (OSINT)
- Blockchain analysis
- Threat intelligence
- Infrastructure reconnaissance
- Data correlation and pattern recognition
- Digital investigation and reporting

Key OSINT Principles
Verify findings using multiple sources, preserve evidence immediately, maintain operational security (OPSEC), and focus only on publicly available information for defensive investigation and awareness efforts.