OSINT Playbook: Tracking Lost Contacts & Deep Web Scans

Generated on: 2025-05-03 15:48:23

# 1. Tracking Lost Contacts

Objective: Locate individuals using publicly available data and intelligent footprinting.

* Step 1: Start with known identifiers (email, phone number, name, username).
* Step 2: Use email & phone reverse lookup tools (e.g., EmailRep.io, PhoneInfoga).
* Step 3: Cross-check social media handles (Sherlock, Maigret, WhatsMyName).
* Step 4: Search leaked databases (HaveIBeenPwned, Dehashed, IntelligenceX).
* Step 5: Use public record search (TruePeopleSearch, Whitepages, Spokeo for US).
* Step 6: Map locations using Exif data (if images available) or GeoCreepy.
* Step 7: Investigate old domain ownership, WHOIS records, pastebins.
* Step 8: Expand network from known contacts (LinkedIn social graph, Facebook friend lists).
* Step 9: Optional automation using SpiderFoot, Maltego, or Recon-NG modules.
* Step 10: Log every source, time, and findings in Notion for traceability.

# 2. Deep Web Scans

Objective: Explore hidden services and content not indexed by surface search engines.

* Step 1: Setup a secure and anonymous browsing environment (Tails OS or Whonix, with Tor).
* Step 2: Use Dark Web search engines (Ahmia, Not Evil, Kilos, Phobos).
* Step 3: Use Onion.link or Onion.pet bridges for previewing services.
* Step 4: Monitor forums and marketplaces (Dread, Empire, Reddit hidden services).
* Step 5: Access darknet paste sites for sensitive data dumps.
* Step 6: Use dark web scraping tools (OnionScan, TorBot).
* Step 7: Check hidden service directories (Dark.fail, FreshOnions).
* Step 8: Use fingerprinting to identify reused usernames or aliases.
* Step 9: Validate findings with hash or PGP signature comparisons.
* Step 10: Log onion links, aliases, and source context into Notion templates.