OSINT (Open-Source Intelligence) Checklist

This checklist ensures thoroughness, legality and ethical compliance during investigations.

1_PREPARATION PHASE

Define Objectives

- □ Clarify the target (person, organization, event, or technical system).
- □ Set scope: time frame, geography, and data types (e.g., financial records, social media).

Legal & Ethical Compliance

- □ Review GDPR, CCPA, CFAA, and local laws.
- □ Avoid terms of service violations (e.g., scraping restricted sites).
- □ Adhere to ethical guidelines (no doxxing, harassment, or unauthorized access).

Tools & Resources

- □ Prepare tools: search engines, Shodan, theHarvester, SpiderFoot, etc.
- □ Bookmark databases: WHOIS, EDGAR, OpenCorporates, national registries.

Secure Environment

- □ Use VPNs, Tor, or secure browsers (Brave, Firefox with privacy plugins).
- □ Set up a virtual machine (e.g., Kali Linux) for sensitive tasks.

2_DATA COLLECTION PHASE

A. PEOPLE

Search Engines

- □ Advanced operators: site:, filetype:pdf, intitle:, inurl:.
- □ Reverse image search (Google Images, TinEye).

Social Media

- □ Platforms: Analysis across leading social media platforms.
- □ Tools: Social Searcher, Sherlock (username lookup), Holehe (email lookup).

2_DATA COLLECTION PHASE

A. PEOPLE

Emails/Phones

□ Verify breaches: HaveIBeenPwned, DeHashed.

□ Reverse phone lookup: Truecaller, Whitepages.

Public Records

□ Court documents (PACER), property records (Zillow), voter registrations.

□ Genealogy sites: Ancestry, FamilySearch.

B. ORGANIZATIONS

Website Analysis

□ WHOIS lookup, DNS history (SecurityTrails), Wayback Machine archives.

□ SSL certificates (crt.sh).

Financial/Legal

□ SEC filings (EDGAR), business registries (OpenCorporates), sanctions lists.

Employee Data

□ LinkedIn employees, GitHub repositories, conference speaker lists.

C. EVENTS

News/Media

□ Google News, Factiva, local news outlets.

□ Verify viral content: InVID, OSINT Collective online.

Geospatial

□ Google Earth, Sentinel Hub, SunCalc (shadow analysis).

□ Social media geotags and EXIF data (ExifTool).

D. TECHNICAL SYSTEMS

Network Analysis

□ Shodan (IoT devices), Censys, Nmap scans.

□ DNS records (MX, TXT, SPF).

Leaks/Dark Web

□ Pastebin, GhostBin, Tor forums (via OnionScan).

3_ANALYSIS PHASE

Correlation

- □ Cross-reference data (e.g., link phone numbers to social profiles).
- □ Use i2 for relationship mapping.

Credibility Assessment

- □ Check source reputation and biases.
- □ Timestamp verification (e.g., Wayback Machine vs. recent edits).

Pattern Recognition

- □ Identify recurring entities or behaviors across data points.
- □ Look for anomalies or inconsistencies in patterns or formats.

Geospatial Mapping

- □ Overlay data on maps (Google My Maps, QGIS).

4_REPORTING PHASE

Documentation

- □ Screenshots, archived web pages, source URLs.
- □ Structured report: executive summary, methodology, findings.

Credibility Assessment

- □ Encrypt files (VeraCrypt), store in secure drives.
- □ Share via encrypted channels (Signal, ProtonMail).

5_POST-INVESTIGATION ACTIONS

Review Process

- □ Identify gaps (e.g., missed data sources).

Data Retention

- □ Securely delete unnecessary data (BleachBit).

Monitoring

- □ Set alerts (Google Alerts, Mention.com) for ongoing targets.

6_ADDITIONAL CONSIDERATIONS

Training

□ Stay updated via OSINT Curious, OSINT Framework, or SANS OSINT Summit recordings.

Operational Security

□ Use pseudonyms, burner emails, and avoid direct interaction with targets.

Collaboration

□ Share findings with teams via secure platforms (Keybase, SecureDrop).

FINAL TIP

Always verify findings with 2–3 independent sources to counter misinformation. Adapt tools/techniques to the investigation's context (e.g., cybersecurity vs. due diligence).