**📱 Mobile Number Information Gathering Tools**

**🔍 OSINT & Lookup Tools**

1. **Truecaller** – Caller ID & spam detection (web + app).
2. **Sync.me** – Reverse phone lookup and caller identification.
3. **NumLookup** – Free online reverse phone lookup service.
4. **CleverDialer** – Spam protection and caller identification.
5. **Whoscall** – Phone number identification & blocking.
6. **AnyWho** – Online phone directory (mainly for US numbers).
7. **Whitepages** – Reverse phone lookup, address & background checks.
8. **Spokeo** – Phone number lookup, people search, public records.
9. **BeenVerified** – Phone number search with social profiles.
10. **ZabaSearch** – Public record & phone search.

**🛠️ Security & Recon Tools (Kali/OSINT)**

1. **OSINT Framework** – Collection of OSINT tools including phone lookups.
2. **PhoneInfoga** – Advanced tool for scanning phone numbers (Kali Linux).
3. **Maltego** (with plugins) – Link analysis and phone number connections.
4. **Social Analyzer** – Find linked social media accounts from numbers.
5. **Sherlock** – Username search that can link numbers to accounts indirectly.
6. **Holehe** – Check if email/phone numbers are registered on websites.
7. **Creepy** – Geolocation information that sometimes links to phone metadata.
8. **Skiptracer** – OSINT scraping framework (works with numbers, emails).
9. **TheHarvester** – Information gathering that can be combined with phone data.
10. **OSINT-SPY** – Collects various data including phone-related information.

**🌐 Online APIs & Databases**

1. **Numverify API** – Number validation & carrier lookup.
2. **Twilio Lookup API** – Phone validation, carrier & line type detection.
3. **Abstract API (Phone Validation)** – Detects number details & validity.
4. **Google Dorks** – Find leaked phone numbers in public data.
5. **Hunter.io** – Cross-check emails linked to numbers.

## 🔎 Android Mobile Location Tracking Tools (Cyber Security / Forensics)

1. **OSINT Tools for Phone Numbers**
   * **Truecaller** – Identifies SIM/number ownership.
   * **NumVerify / HLR Lookup** – Checks carrier and country info.
   * **PhoneInfoga** – Open-source tool for gathering phone number intelligence.
2. **Android Device Tracking & Monitoring**
   * **Google Find My Device** – Built-in Android tracking.
   * **Cerberus Anti-Theft** – Security & tracking app for lost/stolen devices.
   * **Prey Project** – Open-source device tracker for mobile/laptop.
   * **Where’s My Droid** – Android app for tracking and remote control.
3. **Digital Forensics Tools**
   * **Cellebrite UFED** – Used by law enforcement for extracting GPS/location data.
   * **MSAB XRY** – Mobile forensic suite with location analysis.
   * **Magnet AXIOM** – Extracts location, GPS, WiFi, and cell tower data.
   * **Autopsy with Android Plugins** – Free forensic framework for analyzing location history.
4. **Network & GPS Tracking (Pentesting Tools)**
   * **WiGLE** – Collects WiFi/GPS location data for wireless mapping.
   * **Airodump-ng (Aircrack-ng suite)** – Can gather WiFi APs with GPS mapping.
   * **Kismet** – Wireless network detector with GPS integration.
5. **SIM & Carrier Location Analysis**
   * **OpenCellID** – Community database of cell towers for triangulation.
   * **CellTower Locator Tools** – Help track approximate location by cell tower data.
6. **Malware / Red Team Testing (Ethical Use Only)**
   * **SpyNote (for research)** – Android RAT used in red team demos.
   * **AhMyth Android RAT** – Open-source RAT with GPS tracking features (for lab use).
   * **Metasploit Android Payloads** – Can extract GPS/location if permissions are granted.

## 🔍 Social Media OSINT Tools

### 1. ****Maltego****

* Powerful data mining & link analysis tool.
* Maps relationships across social media, domains, emails, phone numbers.

### 2. ****SpiderFoot****

* Automated OSINT tool.
* Collects data from over 200 sources including social media, IPs, and domains.

### 3. ****Social-Searcher****

* Real-time search engine for social networks.
* Finds mentions of usernames, keywords, hashtags.

### 4. ****OSINT Framework****

* A collection of free resources for social media intelligence.
* Covers Facebook, Twitter (X), Instagram, LinkedIn, TikTok, etc.

### 5. ****Creepy****

* Geolocation OSINT tool.
* Tracks location information from social media posts.

### 6. ****Sherlock****

* Username search tool.
* Finds accounts across 300+ social networks using a single username.

### 7. ****Holehe****

* Checks if an email is linked to social media accounts.

### 8. ****Twint****

* Twitter/X OSINT tool.
* Gathers tweets, followers, mentions without needing Twitter API.

### 9. ****TheHarvester****

* Email, subdomain, username gathering tool.
* Useful for finding accounts linked to emails.

### 10. ****Instagram OSINT Tools****

* **InstaLooter / Instaloader** – download and analyze Instagram profiles.
* **OSINTgram** – extracts followers, hashtags, location data.

### 11. ****Facebook OSINT Tools****

* **FBStalker (archived)** – profile data gathering.
* **Graph Search (via tools like IntelligenceX)** – extract open data from Facebook.

### 12. ****LinkedIn OSINT Tools****

* **LinkedInt / LittleBrother** – gathers employee & company profiles.
* Great for corporate OSINT & reconnaissance.

### 13. ****TikTok OSINT Tools****

* **Tiktok-scraper** – extracts videos, hashtags, user info.
* **SOWED** – social media web data analysis.

### 14. ****Recon-ng****

* Web reconnaissance framework.
* Collects info from multiple OSINT sources including social media.

### 15. ****Google Dorks for Social Media****

* Advanced search queries to extract hidden social profiles & posts.

**WhatsApp-Specific OSINT Tools & Techniques (2025)**

**1. API Link-Based Phone Number Check**

* Use URL formats like https://api.whatsapp.com/send/?phone=NUMBER or https://wa.me/NUMBER. Entering a number here lets you check whether it's registered on WhatsApp quickly—if the number is valid, you'll see a “Continue to Chat” prompt; otherwise, you'll receive a message saying it's invalid.[knowlesys.com](https://knowlesys.com/en/articles/social_websites/whatsapp/whatsapp_open_source_intelligence_investigation_methods.html?utm_source=chatgpt.com)

**2. Profile Picture Extraction**

* Once a number is confirmed, you can access the user’s profile picture by clicking the profile image in WhatsApp Web or opening it in a new tab to extract the URL.[knowlesys.com](https://knowlesys.com/en/articles/social_websites/whatsapp/whatsapp_open_source_intelligence_investigation_methods.html?utm_source=chatgpt.com)

**3. WhatsApp Profile Metadata**

* The “About” section (status message), profile photo, and “last seen” timestamps are rich metadata points. These can be cross-referenced across platforms for identity correlation (e.g. “CFO at TechCorp Hong Kong”) or used to infer user behavior, time zone, or interests.[blog.pagefreezer.com](https://blog.pagefreezer.com/whatsapp-osint-investigation-guide?utm_source=chatgpt.com)

**4. Group Link Discovery**

* Public WhatsApp group links can be found online using targeted Google searches (Google “dorking”), such as:
* chat.whatsapp.com "topic"
* site:instagram.com chat.whatsapp.com "Traders Club"

This helps locate groups related to your investigative subject.[knowlesys.com](https://knowlesys.com/en/articles/social_websites/whatsapp/whatsapp_open_source_intelligence_investigation_methods.html?utm_source=chatgpt.com)[blog.pagefreezer.com](https://blog.pagefreezer.com/whatsapp-osint-investigation-guide?utm_source=chatgpt.com)

**5. Advanced Tools & Automation**

* **WebPreserver**: Capture full chat conversations—alongside media, timestamps, and metadata—in a forensically sound way that may be admissible in legal proceedings.[blog.pagefreezer.com](https://blog.pagefreezer.com/whatsapp-osint-investigation-guide?utm_source=chatgpt.com)
* **Android Emulators** (e.g., BlueStacks, NoxPlayer, MEmu): Use these to run WhatsApp on PC, which facilitates easier capture, media extraction, and reverse image searches.[blog.pagefreezer.com](https://blog.pagefreezer.com/whatsapp-osint-investigation-guide?utm_source=chatgpt.com)

**6. Cross-Platform Correlation**

* Leverage services like Truecaller, reverse phone lookup sites, or Username Finder tools to match a WhatsApp phone number with email, social media profiles, or usernames across platforms.[blog.pagefreezer.com](https://blog.pagefreezer.com/whatsapp-osint-investigation-guide?utm_source=chatgpt.com)

**Broader OSINT Tools Useful for WhatsApp Investigations**

While not WhatsApp-specific, these tools are valuable for gathering supporting intelligence:

* **Maltego** – Comprehensive link analysis and visualization (e.g. mapping phone → social media → organizations).[Wikipedia](https://en.wikipedia.org/wiki/Maltego?utm_source=chatgpt.com)
* **1 TRACE** – A modern, modular web-based OSINT suite offering cross-domain intelligence (SOCMINT, CYBINT, FININT, GEOINT, dark web, blockchain, leaks), well-suited for integrated investigations.[Wikipedia+1](https://en.wikipedia.org/wiki/1_TRACE?utm_source=chatgpt.com)
* **Recon-ng**, **SpiderFoot**, **Shodan**, **TheHarvester**, **Google Dorks**, **Amass**, **ExifTool**, **FOCA**, **ShadowDragon**, **OSINT Framework** – Valuable for infrastructure mapping, metadata extraction, reconnaissance, and username enumeration.[Wikipedia](https://en.wikipedia.org/wiki/List_of_OSINT_tools_and_frameworks?utm_source=chatgpt.com)[PyNet Labs](https://www.pynetlabs.com/osint-tools/?utm_source=chatgpt.com)

**Summary Table: Tools & Techniques**

| **Tool / Technique** | **Purpose** |
| --- | --- |
| API-based URL check | Verify WhatsApp registration via wa.me links |
| Profile picture extraction | Save or inspect WhatsApp avatar |
| Metadata (About, Status, Last Seen) | Gather identity clues, time zones, professional info |
| Google Dork Group Link Discovery | Locate public WhatsApp group chats |
| WebPreserver | Forensically capture full chat content for evidence |
| Android Emulators | Run WhatsApp on PC for easier workflow |
| Correlation Tools | Link phone numbers to other identities across platforms |
| Maltego / 1 TRACE / Recon and more | Deep analysis, mapping, and cross-source intelligence aggregation |

**Ethical & Legal Reminders**

* **Use Only Public Data**: Many of these techniques rely on publicly accessible info or your direct interactions (e.g., via URL).
* **Privacy and Legality**: Always consider regional laws and user privacy. OSINT shouldn’t cross into unauthorized access or surveillance.
* **Avoid Abuse**: Techniques like group infiltration or exploiting metadata must comply with legal frameworks and terms of service.

**ndroid Security & Pentesting Tools**

1. **Drozer** – Android app security assessment framework.
2. **Frida** – Dynamic instrumentation toolkit (for runtime code manipulation).
3. **APKTool** – Reverse engineering Android apps (decode & rebuild APKs).
4. **MobSF (Mobile Security Framework)** – Automated mobile app pentesting framework.
5. **Burp Suite Mobile Assistant** – Proxying and analyzing mobile app traffic.
6. **QARK (Quick Android Review Kit)** – Static code analysis for Android vulnerabilities.
7. **Objection** – Runtime mobile exploration toolkit (powered by Frida).
8. **Dex2Jar** – Convert .dex (Dalvik bytecode) to .jar for decompiling.
9. **JD-GUI** – Java decompiler for analyzing Android apps.
10. **mitmproxy** – Intercept and modify mobile app traffic.
11. **AndroBugs Framework** – Static code analysis tool for Android vulnerabilities.
12. **SMALI/Baksmali** – Disassembler/assembler for Android .dex files.
13. **Xposed Framework** – Modify app/system behavior at runtime.
14. **Wireshark (with Android device)** – Network packet analysis.
15. **CuckooDroid** – Android malware analysis sandbox.
16. **Nmap (with Termux on Android)** – Network scanning tool.
17. **NetHunter (Kali Linux for Android)** – Complete mobile pentesting platform.
18. **Hopper Disassembler** – Reverse engineering tool for Android binaries.
19. **RMS (Runtime Mobile Security)** – Frida-based mobile security testing toolkit.
20. **AppMon** – Automated dynamic monitoring for Android apps.

✅ These are **used by ethical hackers, penetration testers, and researchers** to:

* Test app vulnerabilities
* Analyze mobile malware
* Perform reverse engineering
* Strengthen Android app security

**🔎 Social Media OSINT & Investigation Tools**

1. **Maltego** – Powerful link analysis for mapping social media networks.
2. **Social-Searcher** – Social media search & monitoring.
3. **SocioSpyder** – Open-source social media scraping & analysis.
4. **Creepy** – Geolocation intelligence from social media data.
5. **Twint** – Twitter OSINT scraping (without API).
6. **TweetDeck** – Twitter monitoring and case tracking.
7. **Hoaxy** – Disinformation tracking on Twitter.
8. **Foller.me** – Twitter profile analytics.
9. **Hunchly** – Evidence collection & web capture for social media cases.
10. **Who Posted What?** – Search Facebook posts by keywords & dates.

**🌍 Cross-Platform Social Media Analysis**

1. **OSINT Framework** – Collection of categorized OSINT tools.
2. **SpiderFoot** – Automated footprinting & social media info gathering.
3. **Recon-ng** – Reconnaissance framework for social media and online data.
4. **IntelTechniques** – Social media investigation toolkit.
5. **Social Bearing** – Advanced Twitter analytics.
6. **Echosec** – Social media discovery & geospatial analysis.
7. **Geofeedia** – Social media content location tracking.
8. **Sotrender** – Social media analytics for cases.
9. **CrowdTangle** – Facebook & Instagram monitoring.
10. **Brandwatch** – Large-scale monitoring of mentions across social media.

**📱 Fake Account / Identity Verification Tools**

1. **PimEyes** – Reverse image search for faces.
2. **TinEye** – Reverse image search to track fake photos.
3. **Google Reverse Image Search** – Cross-platform photo investigation.
4. **Yandex Image Search** – Strong reverse image detection.
5. **PhotoForensics** – Image metadata & manipulation check.
6. **EXIF Tool** – Extract metadata from images shared online.
7. **Skiptracer** – Social media & phone number lookup (Python).
8. **Sherlock** – Username search across hundreds of platforms.
9. **Maigret** – Alternative to Sherlock, deeper social profile search.
10. **NameChk** – Check username availability across social platforms.

**🛠 General OSINT Tools Useful in Social Media Cases**

1. **TheHarvester** – Collect emails, names, and accounts linked to social.
2. **FOCA** – Metadata extraction from online docs (can link to social IDs).
3. **ExifTool** – Metadata analysis (photos, videos).
4. **Metagoofil** – Document metadata gathering.
5. **Kali Linux OSINT Tools Pack** – Built-in set of social media tools.
6. **SpiderFoot HX** – Automated online identity analysis.
7. **Google Dorks** – Advanced Google search operators.
8. **Shodan** – Can correlate devices with social media activity.
9. **Pipl** – Deep people search (paid).
10. **BeenVerified** – Identity investigation tool.

⚡ These tools are commonly used by **cybersecurity researchers, digital forensics experts, and OSINT investigators** for:

* Tracking fake social media accounts.
* Collecting intelligence from posts, profiles, and groups.
* Monitoring disinformation or cybercrime activity.
* Building evidence for legal or research cases.