1.1 Identify the Basic Data

Every OSINT inquiry begins with at least one *seed*:

- **Name** – full name, nickname, alias
- **Username/Handle** – Instagram, Discord, forum name
- **Email Address** – work or personal
- **Phone Number** – mobile or VoIP
- **Image** – a photograph, avatar, or logo
- **Location Clue** – city, workplace, school

1.2 Gathering the Starting Handle

Your *seed* might come from:

- A social media profile,
- A comment on a forum,
- A watermark on an image,
- A leaked email address (many emails contain the same "name stem").

If you only have a **partial handle**, keep variations in mind:

- Replace underscores with dots or hyphens.
- Try common number substitutions (e.g., `0` for `o`, `1` for `l`).

1.3 Automated Discovery Tools

Several open-source tools and web services can quickly check a username across hundreds of platforms.
These rely **only on public profile pages** and are legal when used responsibly.

Tool	Type	Key Features
WhatsMyName	Web	Fast checks on 500+ sites with direct profile links
Sherlock	Command-line	Scans hundreds of services; export results
Maigret	Command-line	Similar to Sherlock but includes more niche sites
Namechk / KnowEm	Web	Quick availability search, useful for spotting patterns

Tool	Type	Key Features
Social Analyzer	Python/GUI	Multi-platform checks, some content preview

> ⚠️ **Tip**: Always confirm results manually.
> Automated tools may produce *false positives* if someone else uses the same handle.

🔎 1. General Profile Discovery

Purpose	Example Query	Explanation
Find a username on a specific site	`"username" site:twitter.com`	Exact match of handle on Twitter
Search across multiple networks	`"username" site:instagram.com OR site:facebook.com`	Combines multiple social platforms
Catch hidden mentions	`inurl:profile "username"`	Finds URLs containing “profile” and the handle
Detect account directories	`"username" inurl:members`	Useful for forums and gaming sites

---

🌐 2. Email & Contact Info

Purpose	Example Query
Find an email on a domain	`"name@example.com"`
Guess hidden addresses	`"firstname lastname" email`
Find leaked addresses	`"@gmail.com" "Full Name"`
Company contact pages	`"@company.com" intitle:contact`

🖼️ 3. Images & Avatars

Purpose	Example Query
Find hosted profile pics	`intitle:index.of "username" jpg`
Search social avatars	`"username" filetype:jpg`
Public Google Photos albums	`site:photos.google.com "Full Name"`

🏠 4. Location & Maps

Purpose	Example Query
Check for check-ins	`"username" "checked in at"`
Public location tags	`"Full Name" "lives in" OR "from"`
Old Google Maps contributions	`site:google.com/maps/contrib "username"`

🧵 5. Forums & Archives

Purpose	Example Query
Forum posts	`"username" inurl:showthread`
Old cached content	`cache:example.com "username"`
Pastes & leaks	`"username" site:pastebin.com`
Archived profiles	`site:archive.org "username"`

⚡ Advanced Combinations

Query	Use Case
`"username" AND ("city" OR "nickname")`	Narrow by location or alias
`"Full Name" AROUND(3) "birthdate"`	Finds name within 3 words of a date
`"Full Name" filetype:pdf`	Scans resumes, academic papers, public reports
`"username" ext:csv OR ext:xls`	Finds spreadsheets containing the handle

✅ Tips for Effective Dorking

- Use **quotes** `" "` for exact phrases.
- Use **OR** to combine multiple platforms in a single query.
- Use **site:** to focus on a specific domain.
- Use **AROUND(X)** to locate words close together (e.g., name + city).
- Start broad, then add filters (filetype, date range) to refine.

📧 Email Intelligence Tools

Tool	Type	Key Features	Link
HaveIBeenPwned	Web	Checks if an email appears in known breaches	haveibeenpwned.com
DeHashed	Web (freemium)	Searches breaches, pastes, and hidden services	dehashed.com
IntelX	Web	Paste site archives, darknet leaks	intelx.io
Emailrep.io	API/Web	Email risk scoring, domain reputation	emailrep.io
Hunter.io	Web/API	Finds email formats and contacts for a domain	hunter.io
Clearbit Connect	Browser add-on	Shows email/LinkedIn data from Gmail inbox	clearbit.com/connect
GHunt	CLI	Investigates Google accounts by email (profile photos, calendars if public)	github.com/mxrch/GHunt
SocialCatfish	Web (paid)	Reverse search emails for profiles & images	socialcatfish.com

📱 Phone Intelligence Tools

Tool	Type	Key Features	Link
Truecaller	Mobile/Web	Caller ID & reverse lookup (global)	truecaller.com
Numverify	API/Web	Carrier lookup, line type, country	numverify.com
OSINT Industries Phone Lookup	Web	Free basic carrier/country info	osint.industries
Whitepages	Web (US-centric)	Reverse phone & address search	whitepages.com

Tool	Type	Key Features	Link
Spokeo	Web	Combines public records & directories	spokeo.com
PhoneInfoga	CLI	Open-source scanner for numbers (format, carrier, OSINT queries)	github.com/sundowndev/phoneinfoga
CallerID Test	Web	Quick number validation	calleridtest.com

🔎 Cross-Platform & Multi-Use Tools

Tool	Use Case	Link
Maltego	Visual link analysis of email/phone relationships	maltego.com
SpiderFoot	Automated OSINT collection from many sources	spiderfoot.net
Recon-ng	CLI framework for automated email/phone reconnaissance	github.com/lanmaster53/recon-ng

💡 Practical Workflow Example

1. **Format & Validate** – Use **libphonenumber** or Numverify to confirm country and carrier.
2. **Breach Check** – Run the email in **HaveIBeenPwned** and **DeHashed**.
3. **Username Pivot** – Extract the part before `@` and run through **WhatsMyName** or **Sherlock**.
4. **Risk & Metadata** – Score with **Emailrep.io**, then search Google with queries like:

```
"person@example.com" OR "555-1234" filetype:pdf
```

5. **Visualization** – Import all results into **Maltego** or a spreadsheet to spot relationships.

VISUAL CLUES TO WATCH

- 🌆 **Background Landmarks** – buildings, mountains, unique street art.
- 🌞 **Shadows** – use **SunCalc** to estimate time & location.
- 👥 **Recurring Faces** – friends who appear across platforms reveal networks.
- **Background Forensics**: Feed photos into **SunCalc** or **Google Earth** for geolocation.

More tools. More pivots. Same public-only ethics.

🌐 Platform	Fast Moves	Killer Tools & Resources
Facebook	Public group & event mapping, profile history	**graph.tips**, **Stalkscan** (legacy), **Wayback Machine**, **Hunchly** (case capture), **SearchIsBack**, **PeopleFindThor**
Instagram	Download posts & metadata, hashtag geolocation	**Instaloader**, **Picuki**, **Dumpor**, **Inflact Viewer**, **StoriesIG**, **OSINTgram** (CLI)
Twitter / X	Scrape tweets, followers, timeline analytics	**Twint**, **Snscrape**, **Social Bearing**, **FollowerWonk**, **TweetBeaver**, **BirdHunt**
LinkedIn	Employee graphs, hidden connections, email patterns	**Hunter.io**, **PhantomBuster**, **LittleSis**, **SalesQL**, **LinkedIn Sales Navigator filters**
TikTok	Track trending sounds, user growth, background clues	**Exolyt**, **TokCount**, **Tokscraper**, **OSINT TikTok User Finder**, **VidIQ**
GitHub / GitLab	Extract emails from commits, repo timelines	**GHunt**, Native search + `user@email` dorks, **Gitrob**, **Repo-supervisor**
Reddit	Post history, cross-platform handle reuse	**Pushshift API**, **RedditSearch.io**, **Camas OSINT**, **SnoopSnoo**
Discord	Public server discovery & message capture	**Disboard.org** (server finder), **DiscordLookup**, **dhtscraper**
YouTube	Channel email discovery, comment analysis	**Noxinfluencer**, **ChannelCrawler**, **YouTube DataViewer (Amnesty)**, **Youscan**
Pinterest	Image pivoting to real identities	**Pinsearch**, **ImageRaider**, **Yandex Reverse Image**
Snapchat	Public map & geofenced stories	**Snap Map** (map.snapchat.com), **MapSnapper**, **SCtools**
Telegram	Public group/channel OSINT	**TGStat**, **Telemetr.io**, **TgScan**, **Telepathy**
Mastodon / Fediverse	Decentralized network user hunt	**Fediverse Observer**, **FediFinder**, **FediTips**
Dating Apps (public traces)	Verify profile photos, usernames	**SocialCatfish**, **PimEyes**, **Tineye** (reverse image), **Image Identify**

IMAGE, VIDEO & METADATA ANALYSIS

🖼️ IMAGE INTELLIGENCE

1️⃣ Metadata Extraction

Hidden in every photo can be *EXIF data*: camera model, date/time, GPS.

Tool	Cool Use
ExifTool	The gold standard for pulling EXIF (dates, GPS, camera).
Jeffrey's EXIF Viewer	Quick web check for EXIF/ICC profiles.
Metapicz	Browser-based metadata viewer.
FOCA	Batch-scan entire websites for embedded metadata.

⚠️ **Note**: Platforms like Instagram & Twitter usually strip EXIF, but some smaller sites or direct uploads preserve it.

2️⃣ Reverse Image Search

Find where an image appears elsewhere.

Tool	Superpower
Google Images	Fast, global coverage.
Yandex	Excellent facial recognition & scene matching.
TinEye	Finds earliest known upload, best for version history.
Bing Visual Search	Strong object recognition.
PimEyes (paid)	Face-focused reverse search.
Search4Faces	Russian social network face search.

💡 *Pro Tip*: Crop the image to different sections to trigger different matches.

3️⃣ Photo Forensics

Detect manipulation or edits.

Tool	What it Does
FotoForensics	Error Level Analysis to spot Photoshop.
Forensically	Clone detection, noise analysis, metadata viewer.

Tool	What it Does
Image Edited?	Quick ELA & histogram checks.

🎥 VIDEO INTELLIGENCE

1️⃣ Frame-by-Frame Secrets

- Use **FFmpeg** or **VLC** to extract still frames.
- Run each frame through reverse image search for hidden scenes.

2️⃣ Verification & Analysis

Tool	Key Feature
InVID Verification Plugin	Split video into keyframes, reverse-search them, read metadata.
Amnesty YouTube DataViewer	Pull upload dates and hidden IDs from YouTube videos.
Cortado	Detect deepfakes and tampered footage.

🗺️ GEOLOCATION MAGIC

Images often contain indirect location clues—even when EXIF is stripped:

- 🏙️ **Landmarks & Architecture** – Compare skylines in Google Earth.
- 🌞 **Shadow Analysis** – Use **SunCalc.org** to match sun angle to time/date.
- 🌳 **Flora & Signage** – Plants, license plates, street signs reveal regions.

Tools to Help

Tool	Use
Google Earth / Street View	Landmark matching & ground-truthing.
Mapillary	User-contributed street-level photos.
PeakFinder	Identify mountain silhouettes.
Weather Underground	Verify weather conditions for a given date.