

AI OSINT Prompts Free Starter Set

5 structured prompts to run faster, ethical open-source intelligence investigations with any AI assistant.

Process beats tools

Open-source intelligence is mostly process: knowing what to ask, in what order, and how to verify it. These five prompts turn that process into something you can paste straight into any AI assistant.

Replace the brackets with your subject. **Chain them** — each prompt produces leads for the next. **Verify everything** — an AI can plan and summarise, but it can hallucinate. Treat every output as a lead to confirm, not a fact.

The investigation loop. Every solid investigation moves through five stages. Keep returning to it so you stay structured instead of chasing rabbit holes:

Scope (define the question) → **Collect** (gather from public sources) → **Pivot** (turn each finding into the next lead) → **Verify** (confirm against primary sources) → **Document** (record source, time and confidence). The five prompts below walk this loop once, end to end.

Read this first — ethics & legality

- For authorised, lawful, public-source work only: security research, due diligence, threat intelligence, journalism.
- Use only publicly available information and sources you are permitted to access.
- Respect platform terms and applicable law, including GDPR and local privacy rules.
- If a line of inquiry only serves to locate, intimidate or expose a private person, stop.

Scope → Collect

01

Build an investigation plan

SCOPE · RUN THIS FIRST, EVERY TIME

You are an OSINT analyst. My objective is: [state goal in one sentence]. I am authorised to use public sources only. Produce a structured plan: key questions to answer, the entity types involved (people, domains, emails, infra), the public source categories to check for each, the order to work in, and the risks/assumptions to watch. End with the single highest-value first step.

With OpenOSINT: run the plan and OpenOSINT executes each step against real tools as you go.

If the objective sentence is vague, the rest of the investigation will be too. Make the model commit to one question.

02

Email triage

COLLECT · THE MOST COMMON ENTRY POINT

For the email [email], outline a public-source investigation: what the local-part and domain suggest, where this address may be exposed (breaches, paste sites, public profiles), services it might be registered with, and 3 pivots to identities or accounts. List the checks, not guesses.

With OpenOSINT: runs breach and exposure lookups against live sources for [email].

Force “the checks, not guesses” — it stops the model inventing a confident profile.

Pivot → Verify

03

Username spread

PIVOT · A HANDLE IS A HYPOTHESIS, NOT AN IDENTITY

For the username [username], list the platforms most worth checking, how to tell a true match from a coincidence, and what cross-platform signals (avatars, bios, writing style, timestamps) help confirm the same person controls them.

With OpenOSINT: checks the username across platforms and returns real hits to confirm.

The value is in distinguishing a true match from a coincidence. Same handle ≠ same person.

04

Claim verification

VERIFY · THE PROMPT THAT SEPARATES AN INVESTIGATION FROM A GUESS

Verify this claim using public sources: [claim]. List what would have to be true, the primary sources that could confirm or refute each part, the red flags of fabrication, and a final confidence rating with reasoning.

Most bad OSINT dies here. A claim with a single source is a lead, not a fact. Coincidence is not corroboration.

Document

05

Findings report

DOCUMENT · WHAT MAKES THE WORK CREDIBLE

Turn these raw findings into a clear OSINT report: [paste findings].
Structure it as Summary, Key findings (each with source and confidence), Timeline, Gaps/Unknowns, and Recommended next steps.
Keep claims separated from inferences.

With OpenOSINT: feeds the tool outputs in directly so the report cites real sources.

The Gaps/Unknowns section is what makes a report trustworthy. Saying what you couldn't find signals you didn't make the rest up.

THIS IS THE STARTER SET

Get the full pack

The free set walks the loop once. The full **AI OSINT Prompt Pack** has 30+ prompts across every stage of an investigation, plus the complete methodology and an ethics & legal primer so your work stays authorised.

Scoping & planning · Email investigation · Username & social footprint · Domain & website recon · IP & infrastructure · Phone numbers · Company & org due diligence · Image & location clues · Verification & anti-disinformation · Reporting & documentation

Buy the full pack — \$29

Free & open source: the OpenOSINT framework powers these prompts with live data.
github.com/OpenOSINT/OpenOSINT · openosint.tech