

Forum:[Hack Forums](#)

Thread: [OCCRP's OSINT Playbook for Tracking People Who Don't Want to Be Found](#)

Th3Hulk - October 15, 2026, 8:21 am

OCCRP research director Shaya Laughlin published a breakdown of how their team tracks down people who don't want to be found — starting from something as small as a name, a phone number, or a face in the background of a photo. Here's how the process actually works.

Set up your security before you touch anything. The first rule is to never investigate from your personal accounts, because platforms can suggest your real profile to the very person you're looking into. Instead, create believable sock puppets — matching email, a profession, some activity — and route everything through a VPN. If you skip this, you risk tipping off your subject, which in a criminal investigation can be genuinely dangerous.

Archive as you go. People scrub their digital footprint the moment they sense someone is digging, so capture evidence the instant you find it. Use a full-page screenshot extension with the date and URL visible, save copies to the Wayback Machine, and use tools like Fdown.net for Facebook videos or Story Saver for public Instagram stories. OCCRP learned this the hard way: one colleague investigated the wife of a businessman tied to a sanctioned Cambodian conglomerate, and three years later her entire social media presence was gone — only the screenshots survived.

Start broad before you go deep. Search the person's name and known identifiers on Google using operators like quotation marks for exact matches and the minus sign to cut noise. You can cautiously use AI too, but require cited links and never upload sensitive data. Check archived press databases like LexisNexis and Factiva for old arrests or court appearances. The point is to know what's already public before you start hunting for what isn't.

Then narrow with the right questions. Trying to "find everything on someone" leads to overload. Framing targeted questions — "Is this person related to Official X?" or "What are his ties to Company Y?" — keeps the investigation focused and tells you exactly what evidence you're looking for.

Anchor everything on identifiers, not names. Names are unreliable: transliteration alone turns Mohammed into Muhammad, Mhamad, and a dozen other spellings, and naming structures differ across cultures. What actually confirms identity are dates of birth, email addresses, phone numbers, and usernames, cross-referenced against employment history or family ties.

Pull official records where you can. Run the name through commercial, land, plane, and ship registries. When a country keeps its registry closed — like Venezuela — look for a footprint abroad, such as a U.S. court case that names the person's foreign companies. Government gazettes, public licenses, and DomainTools are all fair game here.

Use third-party databases for leads. OpenCorporates, Equasis, and FlightRadar24 are free starting points, while Sayari, Moody's Orbis, and Offshore Alerts are paid tools that aggregate ownership structures and litigation. Leak databases like ICIJ and OCCRP's own AlephPro can fill the gaps. The catch is that these tools make mistakes, so everything still has to be verified against official sources.

Mine social media through the weakest link. Your subject may have locked-down accounts, but their mother might post publicly every day. Platform choice follows demographics — Boomers on

Facebook, Eastern European millennials on VK. In one case, an OCCRP researcher spent weeks on Instagram chasing a scammer who posed as a Dubai Prince, and it was the scammer's wife who posted a photo of their villa and gave away their location. Reverse image tools like Pimeyes help you trace faces across the web.

Finally, people-search tools turn one clue into a map. OSINT Industries checks an email or phone number against hundreds of sites to reveal linked accounts, while Darkside by District4Labs cross-references billions of leaked dark-web records. Contact-list data is especially useful for common names — entries like "Ahmed from ABC company" or "Joe the electrician" hint at which Ahmed or Joe you're actually looking at. The critical caveat: these tools don't verify ownership of anything. They generate leads, not proof, and because they expose deeply personal data, using them responsibly matters.

The takeaway: digital sleuthing is as much art as science. The tools matter, but curiosity, instinct, and disciplined verification matter more.