OSINT for Investigators

Advanced Techniques Guide

inet-investigation.com

This guide assumes you've mastered the beginner toolkit — Google search operators, state court portals, people search tools, and basic social media searches. These advanced techniques cover the methods used by professional investigators, journalists, and due diligence researchers when standard searches aren't enough.

Who This Guide Is For

Readers who have completed the OSINT Beginner's Guide and want to go deeper. These techniques require more time and judgment than beginner methods but unlock significantly more investigative capability.

1. Advanced Identity Analysis

Building a Complete Identity Picture

Basic searches return names and addresses. Advanced identity analysis goes deeper — linking together fragments from different sources to build a coherent picture of someone's real identity, especially when they're using partial information, aliases, or have a common name.

1 Name Variation Mapping

People appear in records under multiple name formats. Systematic variation searching prevents false negatives.

Generate and search all of these:

- Full legal name: John Michael Smith

- Common variants: John M. Smith, J. Michael Smith, J.M. Smith

- Without middle name: John Smith

- Nicknames: Johnny Smith, Jack Smith (common John nickname)

- Maiden name / former name combinations if applicable

- Misspelling variants for common errors: Smyth, Smithe

Search each variant against court records, business registrations, and property records separately. A judgment filed under 'J. Michael Smith' won't surface in a search for 'John Smith'.

2 Date of Birth Cross-Referencing

DOB is the most reliable deduplication identifier for common names. Use it to confirm you have the right person and to distinguish between two people with identical names.

DOB sources to cross-reference:

- Voter registration records (most states include DOB)

- Court records often include DOB in criminal case headers

- Bankruptcy filings always include full DOB

- Professional license databases frequently include birth year

- People search aggregators use DOB for matching — verify it against primary sources

A DOB that appears consistently across three independent primary sources is highly reliable. If DOBs conflict between sources, you may have two different people or a data error worth investigating.

3	Address History Reconstruction

Reconstructing a full address history — every place someone has lived — is valuable for two reasons: it tells you which court jurisdictions to search, and a timeline of moves can reveal patterns that matter to your investigation (financial distress, relationship changes, evading creditors).

Sources for address history:

- People search tools compile address history from multiple sources — use as a starting map

- Voter registration: each time someone re-registers at a new address creates a record

- Court records: service addresses in civil cases are often personal addresses at time of filing

- Property records: every property purchased or sold

- Bankruptcy filing Schedule J (monthly expenses) often lists current rent/mortgage address

Cross-reference the address timeline against court records: search every county where they lived during the relevant period, not just their current county.

2. Advanced Social Media Investigation

Basic social media searching finds public profiles. Advanced techniques extract location data, reconstruct timelines, and link accounts across platforms even when users have tried to separate them.

4	Geolocation from Social Media Content

Even without explicit geotags, social media posts frequently contain enough visual and contextual information to identify locations.

What to look for in images and videos:

- Street signs, business names, or storefronts visible in background

- Distinctive architecture, landmarks, or geographic features

- Vehicle license plates (first 2–3 characters often visible and jurisdiction-specific)

- Uniform or logo details that place someone at a specific employer

- Time zone clues: posting time relative to stated time zone, daylight patterns

Tools for image geolocation:

- Google Street View: compare background details against street-level imagery

- Google Earth: for outdoor/aerial landmark matching

- SunCalc (suncalc.org): calculate sun position at a given time to confirm location from shadow angle

Systematic geolocation of a series of posts can establish that someone is in a specific city even when they haven't explicitly stated it.

5   Cross-Platform Account Linking

People often try to keep separate identities on different platforms. These techniques identify connections between accounts the subject may believe are unlinked.

Linking vectors to investigate:

- Same username or close variant across platforms

- Same profile photo or variation of it (reverse image search each one)

- Same or similar bio language across platforms

- Same external links in bio (personal website, linktree, etc.)

- Mutual followers/following patterns — accounts following both profiles may indicate the same person

- Posting time patterns: consistent posting hours suggest same time zone and possibly same person

- Writing style and vocabulary patterns across platforms

Start with Sherlock or WhatsMyName to find all accounts under a known username. Then check each account for the linking vectors above.

6   Deleted Content Recovery

Deleted social media posts, profiles, and websites are often partially or fully recoverable through archival and caching services.

Recovery sources:

- Wayback Machine (web.archive.org): historical snapshots of websites and some social profiles

- Google Cache: type 'cache:[URL]' in Google to see the cached version of a page

- CachedView (cachedview.nl): aggregates multiple cache sources

- Twitter/X: deleted tweets sometimes appear in Google's index for weeks after deletion

- Bing News: indexes social content differently than Google — useful secondary cache source

- Screenshots and reposts: search the username plus 'screenshot' or quoted phrases from suspected posts

Archive content you find immediately — it may disappear from caches at any time. Screenshot and record the archive URL, access date, and original URL.

3. Financial and Asset Investigation

Public records contain significantly more financial information than most people realize. These techniques build a picture of someone's assets, debts, and financial history using only free public sources.

7   Bankruptcy Filing Analysis

Bankruptcy filings are among the most information-rich public documents available. They're filed in federal court (searchable through PACER) and contain schedules that disclose:

Schedule A/B — Real and personal property: every asset the debtor owns

Schedule C — Exemptions claimed

Schedule D — Secured creditors: who holds mortgages and liens

Schedule E/F — Unsecured creditors: credit cards, personal loans, medical debt

Schedule I — Current income: employer, pay frequency, monthly income

Schedule J — Current expenses: rent/mortgage, utilities, vehicle payments

Statement of Financial Affairs — recent financial transactions, lawsuits, payments to creditors

A bankruptcy filing provides a more complete financial picture than almost any other public document. Search PACER by name under 'Bankruptcy' court type.

8   Judgment Lien Tracing

When someone loses a civil lawsuit and doesn't pay, the creditor files the judgment as a lien against real property. Tracing these liens reveals both financial disputes and asset locations.

Step-by-step process:

1. Find the underlying judgment in state court records — this shows the amount and original dispute

2. Search the county recorder in every county where the subject owns property for the filed lien

3. Check PACER for federal judgments — these can also be domesticated to state court

4. Search the UCC database at the Secretary of State for personal property liens

Multiple judgment liens from different creditors over a short period is a strong financial distress indicator. The creditor names often reveal the nature of the debts.

9   Hidden Real Estate Research

Property held in LLCs, trusts, or under a spouse's name can obscure ownership. These techniques surface real estate that doesn't appear under a direct name search.

Techniques:

• Search county recorder for LLCs associated with the subject's name or address

• Search Secretary of State for LLCs where the subject is a registered agent or officer

• Search property records by the subject's address to find other properties with the same mailing address

• Search for trust names — living trusts often use the grantor's name (e.g., 'John Smith Living Trust')

• Search for related party names: spouse, business partner, known associates

• PACER bankruptcy Schedules A/B list all real estate interests regardless of how they're titled

Property held in an LLC or trust still has a mailing address on the assessor record — that address often connects back to the beneficial owner.

4. Business and Corporate Investigation

10   Corporate Network Mapping

Individuals who operate multiple businesses — or who want to obscure their involvement in a business — leave traces across Secretary of State records that can be mapped.

Building a corporate network map:

• Search Secretary of State in the subject's home state for all businesses where they appear as officer, director, member, or registered agent

• For each business found, search for other officers/members — who else is involved?

• Search the business's registered address across all states — the same address may appear as registered agent for many entities

• Search other states where the business is registered as a foreign entity

• Check for suspended, dissolved, or revoked business registrations — these indicate activity history

• Search OpenCorporates (opencorporates.com) for cross-state corporate record aggregation

A shared registered agent address is one of the most useful linking vectors — it often connects multiple companies back to the same beneficial owner.

11   Domain and Website Ownership Investigation

Websites and domains can be linked back to their operators through registration records, technical infrastructure, and historical data — even when privacy protection is enabled.

Investigation approach:

• WHOIS lookup (whois.domaintools.com or lookup.icann.org): registrant contact details for older/unprotected domains

• Historical WHOIS (DomainTools): shows registrant details before privacy protection was added

• Reverse IP lookup: find all domains hosted on the same server (often owned by same person)

• BuiltWith (builtwith.com): identifies analytics codes, ad networks, and other identifiers that link sites

• Google Analytics ID: if two sites share the same GA tracking code, they're likely owned by the same entity

• Wayback Machine: historical screenshots of the website, sometimes before contact information was removed

A shared Google Analytics ID or hosting IP address linking two apparently unrelated websites is one of the strongest connecting indicators available through open sources.

5. Documentation and Evidence Standards

For investigations that may support legal proceedings, journalism, or formal due diligence reports, documentation standards matter significantly. Evidence that can't be authenticated or traced back to its source has limited value.

Documentation Best Practices

What to Capture	How to Capture It	Why It Matters

URL of source page	Copy exact URL including parameters	Confirms where information was found
Date and time accessed	Note immediately when found	Web content changes — timestamp matters
Screenshot of page	Full-page screenshot with URL visible	Pages disappear; screenshots preserve them
Archive copy	Submit URL to web.archive.org immediately	Creates independent third-party record
Source description	Note what type of record it is	Establishes reliability level of the source
Search terms used	Document exact queries that produced results	Enables reproduction and verification
Identity confirmation	Note how you confirmed this is the right person	Distinguishes from same-name confusion

Chain of Custody for Digital Evidence

For evidence that may be used in legal proceedings: document every step of collection. Note what you searched, what you found, when you found it, and how you preserved it. Courts are increasingly familiar with OSINT evidence — what they require is that it be traceable, reproducible, and authenticated.

6. Legal Boundaries for Advanced Investigators

Advanced techniques increase investigative capability — and increase the risk of crossing legal lines if applied carelessly. These are the legal boundaries that become most relevant as OSINT practice deepens.

Issue	Legal Line	Consequence
Accessing private accounts	Any access without authorization — even if password is known	Federal + civil CFAA liability
Pretexting	Calling employers, banks, or individuals under false identity to obtain info	Civil + federal crime under GLBA
Aggregating data for employment/housing	Using OSINT findings to make formal decisions without FCRA compliance	Civil FCRA liability
Automated scraping	Most platforms prohibit scraping in ToS; some states enforce legal restrictions	Civil + potential criminal
GPS/tracking device	Installing tracking device on vehicle without consent — illegal in most states	Criminal liability
DMV records	Accessing DMV data without DPPA permissible purpose	**Federal criminal violation**
Sealed/juvenile records	Accessing sealed records through any means	**Criminal contempt + liability**
Using findings to harass	Using locate information to intimidate, stalk, or harass	**Civil + criminal stalking charges**

The Golden Rule of Advanced OSINT

If the information requires you to impersonate someone, access a private system, trick someone into revealing it, or circumvent a privacy protection — stop. The technique is illegal regardless of your purpose or how justified the investigation feels. Stick to what's genuinely public and you stay on solid legal ground.

Further Resources for Continued Learning
These resources are used by professional investigators and journalists to develop advanced OSINT skills:

Resource	URL	What It Offers
Bellingcat	bellingcat.com	Professional investigative OSINT guides and case studies
OSINT Framework	osintframework.com	Comprehensive tool directory organized by category
Michael Bazzell Podcast	inteltechniques.com	Privacy and OSINT techniques from a former FBI investigator
SANS OSINT Summit	sans.org/osint-summit	Annual conference — talks available after the event
TraceLabs	tracelabs.org	OSINT practice through missing persons CTF competitions
Aware Online Academy	aware-online.com	Structured OSINT training courses