

OSINT Investigation Services for Attorneys

Jason Larkin - GI Consulting

October 14, 2025

Contents

OSINT Investigation Services for Attorneys	1
Fast, Cost-Effective Intelligence to Support Civil Litigation	1
Why OSINT Before Subpoenas?	1
Service Value for Legal Practice	2
Case Types We Support	2
Typical Engagement Models	3
Recent Results	4
Process & Timeline	4
Pricing Philosophy	5
Legal & Ethical Standards	5
Firm Benefits	6
How to Engage	6
FAQs for Attorneys	7
Next Steps	8

OSINT Investigation Services for Attorneys

Fast, Cost-Effective Intelligence to Support Civil Litigation

Why OSINT Before Subpoenas?

The Problem

Your client has been harassed by anonymous burner phones and VPN-masked IPs. You need to file subpoenas, but: - **Which targets are worth pursuing?** (Some cost \$5K+ and yield nothing) - **How long will it take?** (Verizon: 3-4 weeks, International: 6-12 months) - **What's the success rate?** (VPN providers: <20%, Domestic carriers: 85%+)

The Solution

OSINT investigation **before** filing subpoenas: - Identify actionable targets in 24-72 hours - Rule out expensive dead ends (international VPNs, Tor nodes) - Provide cost/timeline/success rate estimates for each target - Deliver court-ready reports with evidence documentation

Service Value for Legal Practice

1. Pre-Subpoena Intelligence

What We Do: - Analyze phone numbers (identify VOIP carrier, social media links) - Analyze IP addresses (WHOIS, geolocation, VPN detection) - Cost-benefit analysis (which subpoenas are worth filing)

Value: - **Speed:** Same-day IP intelligence vs. weeks for legal subpoena - **Cost:** Avoid \$2K-5K+ per international subpoena with <20% success rate - **Targeting:** Focus client resources on high-ROI domestic targets

Example: - Client case: 8 IPs identified (5 international VPNs, 1 Google proxy, 2 actionable) - OSINT analysis: \$X (1 week) - Avoided cost: \$25K+ in dead-end international subpoenas - Recommended: 2 domestic subpoenas (\$150 total, 85% success rate)

2. Evidence Gathering & Documentation

What We Do: - Server log analysis and forensic data extraction - Email header analysis and metadata collection - Timeline correlation across multiple sources - Text analysis (harassment scoring, threat detection)

Value: - **Court-Ready:** Professional reports with chain of custody - **Comprehensive:** Multi-source evidence strengthens case - **Visual:** Timeline plots help judges/juries understand patterns

Deliverables: - Executive summary for client presentation - Detailed technical report for opposing counsel - Timeline visualizations (phone, IP, harassment events) - PDF compilation for court submission

3. Expert Witness & Testimony Support

What We Do: - Technical investigation methodology documentation - Deposition preparation and expert witness testimony - Report defense against opposing technical experts - Court presentation of OSINT findings

Value: - **Credibility:** Professional investigator with documented methodology - **Technical Expertise:** Explain VOIP, VPN, IP geolocation to non-technical audiences - **Evidence Strength:** Defend investigation methods under cross-examination

Case Types We Support

Harassment & Stalking

- **Challenge:** Anonymous burner phones, VPN-masked IPs, ProtonMail emails
- **OSINT Approach:** VOIP carrier ID, IP intelligence, text analysis
- **Outcome:** Identify subpoena targets, quantify threat level, timeline evidence

Fraud & Misrepresentation

- **Challenge:** Fake identities, stolen photos, fabricated credentials
- **OSINT Approach:** Social media correlation, reverse image search, credential verification
- **Outcome:** Unmask real identity, document false claims

Employment Disputes

- **Challenge:** Anonymous reviews, disparagement campaigns, IP theft
- **OSINT Approach:** Account correlation, writing style analysis, timeline matching
- **Outcome:** Link anonymous activity to suspected employee

Civil Litigation Support

- **Challenge:** Opposing party's digital footprint, witness credibility
 - **OSINT Approach:** Social media history, public records, contradiction identification
 - **Outcome:** Impeachment evidence, settlement leverage
-

Typical Engagement Models

Model 1: Pre-Subpoena Consultation

Scope: Analyze existing evidence (phone numbers, IPs, emails) and recommend subpoena strategy

Timeline: 2-3 days

Deliverable: Executive summary with subpoena targets and cost/success estimates

Use Case: Client has evidence, needs fast targeting before filing

Model 2: Comprehensive Investigation

Scope: Multi-source OSINT, forensic analysis, timeline correlation, comprehensive report

Timeline: 1-2 weeks

Deliverable: Full investigation report, visualizations, subpoena drafts

Use Case: Complex harassment/fraud case requiring detailed evidence

Model 3: Expert Witness Package

Scope: Full investigation + deposition prep + court testimony

Timeline: 2-4 weeks

Deliverable: Investigation report + expert witness testimony

Use Case: High-stakes litigation requiring technical expert testimony

Model 4: Retainer (Ongoing Support)

Scope: On-demand OSINT support for firm's active cases

Timeline: Monthly retainer

Deliverable: Priority access, discounted rates, regular case reviews

Use Case: Firms with regular OSINT needs across multiple cases

Recent Results

Case 1: Harassment Investigation

- **Challenge:** 6+ months harassment, 4 burner phones, anonymous emails, 8 IPs
- **Timeline:** 72 hours to actionable targets, 1 week to comprehensive report
- **Results:** Identified 3 subpoena targets (\$275 total), ruled out \$10K+ in dead ends
- **Outcome:** Attorney filed within 7 days, case progressing to perpetrator ID

Case 2: Employment Dispute

- **Challenge:** Anonymous Glassdoor reviews, suspected former employee
- **Timeline:** 5 days for writing style analysis and account correlation
- **Results:** Linked reviews to ex-employee via linguistic profiling and timing patterns
- **Outcome:** Settlement negotiations strengthened by documented evidence

Case 3: Fraud Investigation

- **Challenge:** Fake LinkedIn profile, stolen credentials, business impersonation
 - **Timeline:** 3 days for reverse image search and social media correlation
 - **Results:** Identified real person behind fake profile, documented extent of impersonation
 - **Outcome:** Cease & desist effective, criminal referral filed
-

Process & Timeline

Step 1: Initial Consultation (30-60 min, No Charge)

- Case overview and evidence review
- OSINT feasibility assessment
- Scope definition and timeline expectations
- Engagement agreement and pricing

Step 2: Evidence Collection (1-3 days)

- Client provides: phone numbers, IP logs, emails, screenshots
- We analyze: VOIP carriers, IP organizations, social media accounts
- We preserve: Timestamped evidence, chain of custody documentation

Step 3: Investigation Phase (3-10 days)

- Multi-source OSINT analysis
- Forensic data extraction and correlation
- Timeline development and pattern analysis
- Subpoena target identification

Step 4: Reporting & Coordination (2-3 days)

- Executive summary for client presentation
- Detailed technical report for legal team
- Subpoena draft templates (if applicable)

- Direct attorney communication on findings

Step 5: Follow-Up (As Needed)

- Additional analysis based on subpoena responses
- Updated reports with new evidence
- Expert witness testimony preparation

Pricing Philosophy

Transparent & Predictable

- **Fixed-fee quotes** for defined scopes (no surprise hourly bills)
- **Tiered pricing** based on complexity and timeline
- **Volume discounts** for firms with multiple cases
- **Retainer options** for ongoing support

Cost Comparison

Service	Traditional Approach	OSINT Approach
IP Intelligence	Verizon subpoena: \$500, 3-4 weeks	Same-day analysis: Included in investigation
Phone Carrier ID	Multiple subpoenas: \$500+ each	24-48 hours: Included in investigation
International IP	AWS Singapore subpoena: \$5K+, 6-12 months, <20% success	OSINT analysis: Rule out before spending

Result: OSINT investigation saves \$5K-25K in dead-end subpoenas while accelerating timeline by weeks or months.

Legal & Ethical Standards

What We Do (Ethical OSINT)

Public sources only (WHOIS, social media, public databases)
 Verifiable evidence with source documentation
 Chain of custody protocols
 Attorney-client privilege maintained
 Court-admissible reports

What We Don't Do (Illegal/Unethical)

No illegal access or hacking
 No social engineering or phishing
 No impersonation or deception

No privacy violations
No contact with opposing parties

Professional Standards

- Law enforcement methodologies
 - Evidence preservation standards
 - Privacy law compliance
 - Professional investigation protocols
-

Firm Benefits

For Solo Practitioners

- **Access to expertise** without hiring full-time investigator
- **Fixed-fee pricing** fits small case budgets
- **Fast turnaround** meets court deadlines
- **Professional reports** impress clients and opposing counsel

For Small/Mid-Size Firms

- **Scalable support** for multiple cases
- **Retainer discounts** for ongoing relationships
- **Expert witness availability** for high-stakes cases
- **Competitive advantage** in harassment/fraud practice areas

For Referral Sources

- **Attorney referral fee** (industry standard 10-15%)
 - **Co-counsel arrangements** for complex cases
 - **White-label reports** available (your firm name on deliverables)
 - **Client satisfaction** = more referrals to your practice
-

How to Engage

Step 1: Initial Contact

Email: jason@giconsulting.com

Subject: "OSINT Consultation - [Your Firm Name]"

Include: Brief case description, evidence available, timeline needs

Step 2: Consultation Call (30-60 min, No Charge)

- Review evidence and objectives
- Assess OSINT feasibility
- Discuss scope, timeline, pricing
- Answer questions about methodology

Step 3: Engagement Agreement

- Fixed-fee quote for defined scope
- Timeline commitment (rush options available)
- Deliverables specification
- Payment terms (50% upfront, 50% on delivery standard)

Step 4: Investigation Begins

- Evidence handoff (secure transfer)
- Regular updates on progress
- Draft findings review before final report
- Delivery within agreed timeline

Step 5: Follow-Up Support

- Answer questions about findings
- Coordinate with legal strategy
- Additional analysis as needed
- Expert witness testimony (if applicable)

FAQs for Attorneys

Q: How is this different from a private investigator?

A: OSINT focuses on digital/technical intelligence (phones, IPs, social media) vs. physical surveillance. We're technical experts, not PIs. Often complementary services.

Q: Is OSINT evidence admissible in court?

A: Yes. Public source intelligence with documented methodology is admissible. We provide chain of custody and can testify as expert witness.

Q: What if you don't find anything useful?

A: Fixed-fee engagements include "no findings" scenarios. We'll document what we checked and why certain leads were dead ends (still valuable for case strategy).

Q: Can you work under attorney-client privilege?

A: Yes. You engage us as part of legal team, work product is privileged. We never contact opposing parties without your direction.

Q: Do you work on contingency?

A: Generally no (fixed-fee preferred), but we're open to discussing contingency arrangements for high-value cases with strong liability.

Q: How do you handle confidential client information?

A: Secure communication (encrypted email), signed NDAs, attorney-client privilege respected, no case details disclosed without permission.

Q: What if opposing counsel challenges your methods?

A: We document every step, use industry-standard tools, follow law enforcement methodologies. Can defend investigation under cross-examination.

Next Steps

For New Engagements:

Email jason@giconsulting.com with case details for no-charge consultation

For Firm Partnerships:

Let's discuss retainer arrangements and volume pricing for your practice

For Referrals:

We offer industry-standard referral fees and co-counsel arrangements

Professional OSINT investigation services for civil litigation, harassment cases, fraud investigations, and employment disputes. Fast, cost-effective, court-ready intelligence.

GI Consulting

Jason Larkin, Principal

jason@giconsulting.com

Advanced Technology Consulting | Digital Intelligence Services