Case Study: Trade Secrets Investigation

Jason Larkin - GI Consulting

October 14, 2025

Contents

Case Study: Trade Secrets Theft Investigation **1**
Linking Former Employee to Competitor Through Digital Footprint Analysis 1
Executive Summary 1
Background 2
Investigation Approach 2
Deliverables 5
Results & Legal Outcome 5
Key Takeaways 6
Technical Methodology 7
Conclusion 7

Case Study: Trade Secrets Theft Investigation

Linking Former Employee to Competitor Through Digital Footprint Analysis

---

Executive Summary

Challenge: Software company suspected former senior engineer of stealing proprietary code and joining competitor. Attorney needed evidence of data theft and non-compete violation before filing injunction.

Solution: OSINT investigation of social media activity, LinkedIn connections, GitHub repositories, and email intelligence to establish timeline of theft and competitive activity.

Results: Documented 47 unauthorized GitHub commits, LinkedIn job posting dates showing overlap, and social media posts revealing new employment 30 days before resignation. Company won preliminary injunction and $2.3M settlement.

Timeline: 5 days from engagement to comprehensive evidence package

---

Background

Client Situation

- **Client:** Mid-size software company (150 employees)
- **Subject:** Senior software engineer (7 years tenure)
- **Allegation:** Theft of proprietary algorithms and customer lists
- **Evidence:** IT logs showing unusual file access 2 weeks before resignation
- **Legal Strategy:** Seek preliminary injunction + damages for trade secret misappropriation

Business Impact

- **Competitor announcement:** New product launch with suspiciously similar features
- **Customer defection:** 3 major clients moved to competitor within 30 days
- **Financial exposure:** $5M+ in R&D investment at risk
- **Timeline pressure:** Competitor product launch in 60 days

Attorney Challenge

- **Non-compete clause:** 12-month restriction, 50-mile radius
- **Weak IT evidence:** File access logs but no proof of exfiltration
- **Need:** Establish timeline of theft + new employment + data transfer
- **Timeline:** 1 week to file preliminary injunction before product launch

---

Investigation Approach

Phase 1: Social Media Timeline Analysis (Days 1-2)

Objective: Establish timeline of new employment and relationship with competitor

Methods: - LinkedIn profile archaeology (cached versions, connection dates) - Twitter/X timeline analysis (deleted posts via archive sites) - Facebook check-ins and photo metadata - Instagram location tags and friend connections

Findings:

Platform	Evidence	Timeline Significance
LinkedIn	Connected with competitor CTO	6 months before resignation
LinkedIn	Endorsed by competitor engineers	4 months before resignation
Twitter	Deleted tweet: "Excited for new chapter!"	2 weeks before resignation (deleted day after)
Instagram	Check-in at competitor's office building	3 weeks before resignation

Platform	Evidence	Timeline Significance
Facebook	Photos with competitor employees at industry conference	5 months before resignation

Key Finding: Social connections and physical presence at competitor location established **90 days before** resignation, violating non-compete "preparation" clause.

Evidence Strength: STRONG - Timestamped, archived, court-admissible

---

Phase 2: GitHub and Code Repository Analysis (Days 2-3)

Objective: Document unauthorized code commits and repository access

Methods: - GitHub public profile analysis (commits, repos, stars) - GitLab/Bitbucket cross-platform search - Code similarity analysis (public repos vs. client's proprietary code) - Commit timestamp correlation with work hours

Findings:

Unauthorized Activity: - **47 commits** to personal GitHub repo during work hours (client IP range) - **Repository name:** "ml-customer-segmentation" (matches client's proprietary project name) - **Commit messages:** References to client's internal project codenames - **Code patterns:** Variable names matching client's coding standards

Timing Pattern: - **Spike in activity:** 30 days before resignation (200% increase in commits) - **Final commits:** 3 days before resignation announcement - **Repository made private:** 1 day after resignation (but archived copies obtained)

Technical Analysis: - **Code similarity:** 73% match with client's proprietary algorithms (AST comparison) - **Comments:** Internal client references ("per Mike's requirements" - Mike = client CTO) - **License:** Incorrectly labeled as "MIT" (client code is proprietary/confidential)

Evidence Strength: CRITICAL - Direct proof of code theft with timestamps and similarity analysis

---

Phase 3: Professional Network Intelligence (Day 3-4)

Objective: Map connections between subject, competitor, and intermediaries

Methods: - LinkedIn 2nd/3rd degree connection analysis - Mutual connections identification - Job posting timeline analysis - Professional conference attendance correlation

Findings:

Network Map: - **Subject** connected to **Competitor CTO** (6 months before resignation) - **Competitor CTO** previously worked at same company as **Subject** (8 years ago) - **3 mutual connections** moved from client to competitor in past 18 months - **Subject's LinkedIn profile** showed "Open to Work" badge (4 months before resignation)

Job Posting Analysis: - Competitor posted "Senior ML Engineer" position: 5 months before subject's resignation - Job description: 78% match with subject's resume (specialized skills) - Posting removed: 1 week after subject's resignation (suggesting filled) - Competitor's press release: "Key technical hire" announcement 45 days after resignation

Evidence Strength: STRONG - Establishes premeditation and coordinated recruitment

---

Phase 4: Email and Communication Intelligence (Day 4-5)

Objective: Identify email addresses and potential communication channels

Methods: - Email permutation testing (john.doe@competitor.com, jdoe@, etc.) - Data breach database searches (Have I Been Pwned, Dehashed) - Email header analysis from publicly available sources - VOIP phone number correlation

Findings:

Email Intelligence: - **Personal Gmail:** Subject used same email for GitHub, LinkedIn, and personal projects - **Data breach exposure:** Email appeared in 3 data breaches with password hashes - **Email pattern:** Subject's personal email found in competitor's SSL certificate (technical contact) - **VOIP number:** Subject registered new VOIP number 60 days before resignation (not used for client contact)

Communication Timeline: - **Email address creation:** Subject registered firstname.lastname@competitorname (discovered via DNS enumeration) 45 days before resignation - **Calendar inference:** LinkedIn "busy" status changes correlate with competitor's all-hands meeting times - **Timezone analysis:** Subject's GitHub commits shifted to competitor's HQ timezone 30 days before resignation

Evidence Strength: MEDIUM-STRONG - Circumstantial but highly correlated with theft timeline

---

Phase 5: Document Metadata and Digital Forensics (Day 5)

Objective: Analyze publicly available documents for metadata leakage

Methods: - Competitor's public documentation metadata extraction - PDF/Word document author field analysis - Timestamp and software version correlation - File naming convention analysis

Findings:

Metadata Analysis: - **Competitor's product whitepaper** (published 90 days after subject joined): - Document author: Subject's full name - Software version: Matches client's licensed software versions - Internal document paths: Reference client's server names - Creation date: 2 weeks after subject's resignation

File Naming Patterns: - Competitor's technical docs use identical naming convention to client's internal standards - Example: "CUST_SEG_v2_final_FINAL" (client's naming pattern for customer segmentation)

Evidence Strength: CRITICAL - Smoking gun metadata proving direct document transfer

---

Deliverables

Timeline Visualization

- Social media activity timeline (6 months pre-resignation to 3 months post)
- Code commit activity (1 year span showing spike pattern)
- Employment overlap chart (client employment + competitor activity)
- Network connection map (subject → competitor via mutual connections)

Technical Reports

1. Social Media Intelligence Report (15 pages) - LinkedIn profile evolution (archived versions) - Social connections timeline - Location check-ins and conference attendance - Deleted content recovery (Twitter, Facebook)

2. Code Repository Analysis (22 pages) - GitHub commit timeline with metadata - Code similarity analysis (AST comparison) - Repository naming and description patterns - Commit message analysis (internal references)

3. Professional Network Map (8 pages) - Connection analysis (1st, 2nd, 3rd degree) - Job posting timeline correlation - Competitor recruitment pattern documentation - Industry conference attendance overlap

4. Email and Communication Intelligence (12 pages) - Email address identification and verification - Data breach exposure analysis - VOIP phone number correlation - Communication timeline inference

5. Document Metadata Forensics (10 pages) - PDF/Word metadata extraction - Author field analysis - Software version correlation - File naming pattern comparison

Executive Summary for Attorney (5 pages)

- Key findings with evidence strength ratings
- Timeline of theft and competitive activity
- Recommended legal strategy (injunction + damages)
- Evidence admissibility assessment

Results & Legal Outcome

Preliminary Injunction Hearing

- **Attorney filed:** 7 days after receiving OSINT report
- **Evidence presented:** Timeline visualization, GitHub commits, metadata analysis
- **Judge's ruling:** Granted preliminary injunction (product launch halted)
- **Basis:** "Clear and convincing evidence of trade secret misappropriation and bad faith"

Settlement Negotiation

- **Competitor response:** Immediate settlement discussions after injunction

- **OSINT impact:** Metadata evidence eliminated competitor's defense
- **Settlement terms:**
  - $2.3M payment to client
  - Subject termination from competitor
  - 5-year non-compete extension
  - Public statement retracting product claims

Evidence Strength in Court

- **GitHub commits:** Admitted without challenge (timestamped, authenticated)
- **Document metadata:** "Smoking gun" per judge's statement
- **Social media timeline:** Established premeditation and bad faith
- **LinkedIn analysis:** Showed recruitment pattern and intent

---

Key Takeaways

For Attorneys

1. OSINT Before IT Forensics - Social media and public repositories often reveal more than internal IT logs - Metadata analysis can prove document theft even without file transfer logs - Timeline correlation across platforms establishes intent

2. Speed Advantage - 5 days for comprehensive OSINT vs. 3-6 weeks for traditional computer forensics - Real-time evidence preservation (archived social media before deletion) - Faster time to injunction = better business outcome

3. Cost Efficiency - OSINT investigation: $6,500 - Avoided forensic imaging: $15,000-25,000 (and weeks of delay) - Settlement value: $2.3M - **ROI:** 350x return on investigation investment

For Investigators

1. Multi-Platform Correlation - No single platform tells full story - GitHub + LinkedIn + social media = comprehensive timeline - Metadata analysis provides technical "smoking gun"

2. Archived Content Recovery - Wayback Machine, Google Cache, archive.today for deleted content - Social media "memories" features reveal historical posts - DNS/SSL certificate history shows email addresses

3. Professional Network Mapping - LinkedIn connections reveal recruitment patterns - Conference attendance shows pre-resignation relationships - Job posting analysis establishes timeline of planning

For Corporate Clients

1. Evidence Preservation - Don't confront employee before OSINT investigation (risk of deletion) - Preserve IT logs but don't rely solely on internal forensics - Monitor public repositories and social media during employment

2. Non-Compete Enforcement - OSINT can prove "preparation" during employment (key for enforceability) - Social media check-ins establish physical presence at competitor - Timeline evidence defeats "I started looking after resignation" defense

3. Preventative Measures - Monitor employee GitHub activity for company-related commits - Social media monitoring for competitor connections (HR flag) - Exit interviews with social media disclosure requirements

---

Technical Methodology

Tools & Techniques

Social Media Analysis: - LinkedIn Sales Navigator (connection timeline, profile changes) - Wayback Machine (archived profile versions) - Twitter Advanced Search + archive sites (deleted content) - Instagram location data export - Facebook Graph Search (historical check-ins)

Code Repository Analysis: - GitHub API (commit history, repository metadata) - GitLab/Bitbucket cross-platform search - AST-based code similarity tools - Commit timestamp analysis scripts

Network Intelligence: - LinkedIn scraping (within ToS limits) - Mutual connection mapping tools - Job posting aggregators (historical data) - Conference attendance databases

Email & Communication: - Email permutation tools - Data breach databases (HIBP, Dehashed) - DNS enumeration for email discovery - VOIP number reverse lookup

Metadata Forensics: - ExifTool for document metadata extraction - PDF analysis tools - Microsoft Office metadata viewers - File naming pattern analysis scripts

Legal & Ethical Standards

- **Public sources only:** No illegal access to private accounts
- **Terms of Service compliance:** LinkedIn, GitHub scraping within limits
- **Chain of custody:** Timestamped evidence with source URLs
- **Admissibility:** All evidence court-tested and admitted without challenge

---

Conclusion

OSINT investigation provided fast, cost-effective evidence of trade secret theft that traditional computer forensics would have taken weeks longer to uncover. The combination of social media timeline analysis, GitHub code commits, and document metadata created an irrefutable case that led to successful preliminary injunction and $2.3M settlement.

Key Success Factors: **Speed:** 5 days to comprehensive evidence package (vs. weeks for traditional forensics)
Cost: $6,500 investigation (vs. $15K-25K for imaging and analysis)
Evidence: Multiple corroborating sources (GitHub, social media, metadata)
Outcome: Preliminary injunction granted, $2.3M settlement within 90 days

---

This case study is a composite of common trade secret theft scenarios. Technical methods and results are representative of actual OSINT investigations.

GI Consulting | Professional OSINT Investigation Services
jason@giconsulting.com