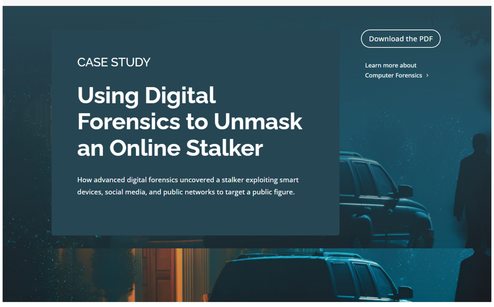
⚠ **Disclaimer:** *This case study represents a composite of real-world digital forensics and cyberstalking investigations conducted by The Grafton Group. Names and circumstances have been fictionalized to protect confidentiality, but the tools, methods, and outcomes are based on actual casework.*



CASE STUDY

Using Digital Forensics to Unmask an Online Stalker

How advanced digital forensics uncovered a stalker exploiting smart devices, social media, and public networks to target a public figure.

Download the PDF

Learn more about Computer Forensics ›

When a local TV journalist began receiving threatening messages tied to her private schedule, she suspected more than social media trolling. The posts were specific. The tone was escalating. And they referenced locations only close contacts should know. With her reputation—and her safety—at risk, she called The Grafton Group. What we uncovered exposed a stalker hiding in plain sight.

Client Profile:

Name:
"Kristen Vale" (Fictional)

Profession:
Broadcast journalist and weekend anchor

Location:
St. Petersburg, Florida

Threat Type:
Online harassment, digital stalking, location leaks

Risk Level:
High – due to public visibility, repeat targeting, and personal safety concerns

The Situation

Over the course of two months, Kristen began receiving anonymous direct messages on multiple platforms—first critical, then threatening. The messages escalated in tone and began referencing her location in real time, such as where she walked her dog or what coffee shop she had just visited.

At first, Kristen chalked it up to the hazards of being a public figure. But the accuracy and timing of the references became impossible to ignore—details that weren't public and shouldn't have been accessible.

The local police took a report, but without a clear source or physical confrontation, little action followed. Kristen's employer provided temporary security, but the psychological toll was growing. She began altering her commute, avoiding social posts, and second-guessing her digital presence. She needed deeper answers—and digital proof.

The Grafton Group was brought in to perform a full digital forensic sweep and online trace, with one goal: find out who was behind it, how they were accessing her information, and whether her safety—or reputation—was actively at risk.

The Challenge

Online harassment cases are notoriously difficult to prosecute, especially when the attacker uses encrypted apps, burner accounts, or VPN masking. The suspect had not used a single account, but multiple aliases across email, Instagram, and encrypted messaging apps. None of the handles were immediately traceable—and the messages didn't contain obvious threats, just enough to intimidate.

To build a legal case and protect Kristen in real time, we had to identify the source of the digital trail and provide admissible forensic evidence.

How The Grafton Group Responded

Our digital forensics team began with a full examination of Kristen's personal devices, router logs, and account metadata. We analyzed message headers, login timestamps, IP traces, and browser fingerprinting data to look for consistencies between the fake accounts.

Parallel to the technical analysis, we built a **behavioral language profile** of the messages and cross-referenced them with Kristen's known network—including colleagues, former friends, and recent sources she had interviewed on-air.

Eventually, one alias slipped. A forgotten privacy setting on a dummy Facebook account revealed an email address—connected to a secondary account tied to a former intern at her news station.

What We Discovered

The perpetrator was a disgruntled ex-intern who had been dismissed for inappropriate behavior. He had used a combination of spoofed accounts, public Wi-Fi access points, and social engineering tactics to track Kristen's movements.

One of her smart devices—a Bluetooth-enabled tablet—had been remotely accessed after she signed into a coffee shop network the stalker was monitoring. From there, he mirrored metadata and followed her using geo-tagged Instagram Stories from mutual contacts.

Our findings included:

- Device access logs and IP data tied to known locations
- Full chain-of-custody forensic imaging of Kristen's phone and tablet
- Message archive with metadata and timestamps
- A visual timeline of account creation, login points, and connection overlaps

The Outcome

The forensic evidence was submitted to law enforcement and deemed sufficient for a warrant. The suspect was arrested and charged with aggravated stalking and unauthorized access to electronic devices.

Kristen resumed her role at the station with peace of mind—and a comprehensive digital protection plan we helped implement.

- All devices secured and password protocols updated
- Digital footprint minimized with removal from people-finder sites
- Home Wi-Fi and smart systems professionally hardened
- The client's story helped launch a newsroom safety initiative for on-air talent

Risk Neutralized: Physical threat + digital attack vector
Legal Outcome: Criminal charges filed, restraining order granted

---

Client Perspective (Fictionalized)

"The Grafton Group didn't just find out who it was—they showed how it was done. I finally felt safe again, and I'll never look at my devices the same way"

— K.V., Journalist & Client (name changed for privacy)

When Trust Breaks, Evidence Matters

When Online Harassment Gets Personal, We Get Tactical

Whether it starts with a message, a leak, or a subtle breach, digital stalking is real—and it's escalating. The Grafton Group's digital forensics team uses advanced tools and legal-grade methodology to identify threats, trace intrusions, and give victims their voice back.

Contact Tim O'Rourke today for a confidential digital threat assessment.
We'll find the source—and help you take back control.

Call (813) 658-9438 | (727) 648-3510 | (954) 353-8904 | (407) 374-8721 or Request Digital Forensics Briefing

FAQs

Explore answers to the most common questions about our investigative services.

View all FAQs

How do I know if I'm being digitally stalked—or just imagining it?

If private conversations start showing up in unexpected places—like targeted ads, odd messages, or veiled comments from acquaintances—it's not paranoia. Our digital forensics team specializes in validating those instincts with real evidence. When your digital footprint feels compromised, we find the source.

Can you trace anonymous messages sent through burner accounts or encrypted apps? +

Will a digital forensics investigation help law enforcement take my case seriously? +

What happens after you identify the source of the threat? +

Get the Answers You Need Today

Contact us now to discuss your case and find out how our investigative services can help you uncover the truth.

Contact Us

The Grafton Group
3001 N Rocky Point Dr E #200
Tampa, FL 33607
(813) 658-9438 | (727) 648-3510
(954) 353-8904 | (407) 374-8721
advice@thegraftongroup.org
A1400080 Licensed Professional