Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/corporate-cyber-espionage-can-be-a-major-league-headache-for-any-business/

CORPORATE ESPIONAGE

Proving Unauthorized Access in Corporate Espionage and Trade Secret Litigation

A rival who knows your bid pricing, formulas or roadmap before you launch often reached them through a system that kept a record of the access. Preserve that record first, put counsel and an examiner on the same call, and decide on any confrontation afterward. Call (800) 868-8189 at any hour.

Published June 22, 2015 · Updated October 30, 2026

Primary Reference for This Guide

Start with NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response.

By Robert Knudsen, Computer forensics and cybersecurity examiner, Global Digital Forensics

When a Competitor Knows Your Pricing or Roadmap Before Launch

Few events threaten a company market position more acutely than discovering that a rival somehow obtained confidential bid pricing, proprietary manufacturing formulas, unreleased source code or strategic M&A targets. Corporate espionage rarely looks like a movie heist. In the digital world, it happens when a competitor recruits an insider prior to resignation, abuses shared vendor credentials to log into a customer portal or deploys targeted spear phishing to monitor executive communications during a critical contract tender.

Tracing the Technical Trail for DTSA Injunctions and Damages

Winning a federal Defend Trade Secrets Act lawsuit, a Computer Fraud and Abuse Act claim or an unfair competition injunction calls for documented technical evidence rather than circumstantial suspicion. Global Digital Forensics performs comprehensive digital examinations, database access audits and SourceScan code comparisons directly for retained litigation counsel and corporate general counsel. Our examiners correlate VPN authentication logs, cloud download telemetry, database query records and endpoint USB and browser artifacts to trace who accessed your proprietary assets, when files moved and how they were transferred. That is the same evidentiary discipline behind our work in Rogers v. BNSF Railway, where the district court entered a 228 million dollar judgment before later ordering a new trial limited to damages.

© 2026 Global Digital Forensics, Inc. All rights reserved.

What the Access Record Shows, and How It Is Corroborated

Counsel usually arrive with a conclusion already formed: the competitor has our numbers, so someone took them. The examination has to be built the other way around, from what the systems recorded toward whoever the record points at. Enterprise systems are better at this than most executives expect. A SharePoint or Google Drive tenant logs every file opened, downloaded, shared and synced by account, timestamp and client IP address. A VPN concentrator records who authenticated, from where and for how long. A customer portal reached through shared vendor credentials still records the source address and browser fingerprint behind each session. On the endpoint, Windows keeps shellbags, Jump Lists, LNK files, the SRUM database and USBSTOR registry keys that together describe which folders a user browsed, which files were opened and what removable media was attached. Those records are where the examiner reads access, timing and the movement of specific files, with a precision that can support an injunction motion.

The report states the reach of each record plainly. A download event shows that a file left the tenant, and the destination devices and accounts are where the examiner follows it next. A USB serial number shows a device was attached, and file system artifacts on that device or on the host are where the examiner looks for a copy. Where credentials were shared, the access record identifies a login, and tying it to a person combines that login with badge records, workstation artifacts, mobile location data or the account holder's own admissions. We set out what each artifact establishes, what inference it supports and which further source would confirm it. That discipline lets counsel argue each point at its true strength, and it is the reason courts have accepted our work as analysis rather than advocacy.

What counsel receive from this part of the work is a timeline rather than a verdict. Each entry places an event, the artifact that records it, the system clock it came from and any correction for time zone or clock drift, so that a download at 11:52 p.m. in the cloud log and a USB connection at 11:54 p.m. on the laptop can be shown to describe the same two minutes. Where two sources disagree, the timeline says so and explains which is more reliable and why. That format lets counsel see the strength of the inference at each step, decide what the demand letter or the motion can safely assert, and prepare the witness who will later explain the sequence to a judge who has never heard of a shellbag.

Misappropriation Under the DTSA and the Evidence Each Element Needs

The DTSA is where most of this work ends up, and its definitions shape the examination from the first day. Under 18 U.S.C. 1839, misappropriation includes "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means", and improper means "includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means" while expressly excluding reverse engineering and independent derivation. Each phrase maps to a forensic question. Acquisition means we tie specific files to specific access events. Improper means often turns on whether the actor exceeded what the confidentiality agreement or the system permissions allowed. The exclusion for independent derivation is the defense we expect, and it is why the examination documents the competitor's access path rather than only the similarity of the result.

© 2026 Global Digital Forensics, Inc. All rights reserved.

The statute also gives counsel a tool that depends almost entirely on forensic readiness. Section 1836(b)(2) allows a court, on ex parte application and "only in extraordinary circumstances", to order seizure of property necessary to prevent the propagation or dissemination of the trade secret. Judges grant that relief when the application shows with specificity what was taken, where it now resides and why ordinary notice would lead to its destruction. An examiner's declaration describing the download telemetry, the destination device and the deletion or wiping activity already observed is what gives the application that specificity. The same showing supports the more common temporary restraining order and the motion for expedited discovery. Our role is to make the technical facts concrete enough that the court can act on them, and we keep the declaration to what the record supports so it is ready for the adversary's own expert.

How an Espionage Engagement Runs From First Call to Report

The engagement begins with scoping under the direction of counsel, because privilege questions and the preservation duty both attach at that moment. In the first conversation we identify the trade secret material by file, repository, database table or folder, the authorized population who could reach it, and the systems that would have recorded the reach. Preservation follows immediately. We export the Microsoft Purview unified audit log or the Google Workspace audit records before retention windows close, snapshot the relevant mailboxes and cloud drives under a litigation hold, pull VPN and firewall authentication logs, and forensically image the endpoints of the people inside the access population, quietly where counsel so directs. Each preservation step is documented with hash values and a chain of custody form, so the integrity of the evidence is documented at every step from collection to courtroom.

Analysis is where the correlation happens. We align the cloud download events against the endpoint artifacts, the USB history against file system timestamps, and the VPN sessions against badge records and travel calendars. When a competitor's product or bid is in hand, we compare it against the protected material, and where source code is involved SourceScan and our source code experts handle the comparison under the protective order. The output is a written report that walks from each artifact to each finding with the exhibits attached, and a declaration shaped to the motion counsel is filing. Robert Knudsen leads the computer forensics work and has supported hundreds of examinations in federal and state matters. The method is the one described in our digital forensics process guide, and it is the same for every client, whatever its size.

Steps That Strengthen a Trade Secret Case From Day One

The most valuable step is preserving the record before anyone confronts the suspected insider or the competitor. A departing engineer who learns of the suspicion may empty personal cloud accounts, reset phones or run wiping utilities, and while those actions leave traces of their own, quiet preservation beforehand captures the content itself. The second is leaving the live systems to the examiner. Each time an administrator logs into the suspect's laptop, opens the files in question or searches the mailbox, new timestamps and access events are written, so the examiner images first and the review works from the copy. The third is exporting the session logs tied to shared vendor credentials and then rotating the credentials, because those logs are often the link between a portal login and a specific outside party.

Equally valuable is defining the trade secret with specificity early. Counsel need a list of the files, formulas, customer records or code modules at issue, and the examination needs the same list to search for, so the two efforts should be joined from the first call rather than reconciled later. Retention windows set the pace. Cloud

© 2026 Global Digital Forensics, Inc. All rights reserved.

audit logs on standard licensing tiers expire in months, and firewall logs often roll over in weeks, so preservation runs from the first day while the business decides its next move. Our guide to common digital evidence mistakes covers the broader pattern. The practical rule is simple: preserve first, under counsel, quietly, and let the analysis determine whether a confrontation, a demand letter or an emergency motion comes next.

Protect Your Competitive Advantage With Immediate Forensic Preservation

If you suspect competitive espionage or unauthorized access to proprietary systems, keep the files exactly as they are so the suspects see no change. Call Global Digital Forensics 24/7 at (800) 868-8189 to coordinate a forensic examination under the direction of counsel. The initial consultation is free.

What the Access Record Shows and How It Is Read

The examination builds the case from what the systems recorded toward whoever the record points at. This table lists the artifacts an espionage examination correlates, what each establishes and how the examiner corroborates it, so counsel can argue each point at its true strength. Read the last column closely, because a download shows a file left the tenant and the next source follows where it went, and a login made with shared credentials is tied to a person through corroboration.

Access artifacts in a corporate espionage matter, what each establishes and how it is corroborated.

Artifact	What it establishes	How it is corroborated
SharePoint or Drive activity log	Files opened, downloaded, shared and synced by account	Exported within retention, 180 days or about six months by provider
VPN concentrator log	Who authenticated, from where and for how long	Tied to a person through device and badge records
Customer portal session record	The source address and browser behind a session	Matched to the vendor's own workstation records
USBSTOR registry keys	A removable device with a serial was attached	File system artifacts checked for a copy
Shellbags, jump lists and LNK files	Which folders were browsed and files opened	Paired with logins and badge records for the user
SRUM database	Application and network resource use over time	Read alongside other artifacts as an estimate
Badge and travel records	Where a person was at a time	Corroborate the login records

The worldwide intellectual property case study describes tracing a customer database and proprietary files emailed to home computers across mail servers, backups and the database itself, the access to movement chain this guide assembles under counsel.

© 2026 Global Digital Forensics, Inc. All rights reserved.

How to Begin and What Happens on the First Call

Before the call, our Insider Threat Checklist: Hold the Accounts, Seal the Laptop sets out the items to secure in the order they expire. Before you call, gather what you can while leaving the suspect systems untouched: the names and roles of the people who could reach the protected material, the systems that hold it, the date the suspicion arose and any letter, bid or product that revealed the leak. In the first conversation the examiner asks what the trade secret is, who had authorized access, what IT or HR has already done, which cloud platforms and licensing tiers are in use and whether litigation counsel is engaged. Afterwards counsel receive a written scope describing the preservation steps, the analysis phases and the timing, together with a proposal for the engagement. The initial consultation is free, and the hotline at (800) 868-8189 answers 24/7.

Technical References and Further Reading

Earlier reporting on this subject: The New York Times on the St. Louis Cardinals and Houston Astros database intrusion, June 16, 2015 and Sports Illustrated on the same case, June 18, 2015.

Authorities cited in this guide: 18 U.S.C. 1839, Definitions (Defend Trade Secrets Act). Defines misappropriation and improper means, including the exclusion for reverse engineering and independent derivation, as currently codified at Cornell LII. 18 U.S.C. 1836, Civil proceedings. Establishes the private right of action and the ex parte seizure remedy available only in extraordinary circumstances, current codified text. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response. Describes the collection, examination, analysis and reporting phases that structure the engagement, final version published 2006. Microsoft Learn, Manage audit log retention policies. Documents how long Microsoft 365 audit records are kept by license level, current Microsoft documentation.

FREQUENTLY ASKED

Questions Counsel and Security Leaders Ask About Corporate Espionage

Can you tell if a competitor hired our former employee to take files?

The record can show what the employee accessed, downloaded and moved before leaving, and when a personal account or device received it. Whether a competitor induced that conduct is usually established through the competitor's own records in discovery, through timing that lines up with recruitment contacts in the employee's email and messages, and through the appearance of the material in the competitor's bids or products. We document the technical chain and the timing. Counsel build the inducement case on top of it, often with expedited discovery that the forensic declaration supports.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Can access through a shared vendor login be traced to one person?

Often, through correlation across several records. The portal records the source IP address, the browser and operating system fingerprint and the session times. We compare those against the vendor's own VPN or workstation records, the user agent strings tied to known devices, and any files the session touched that later appear elsewhere. When the vendor cooperates, workstation artifacts settle the question quickly. Without that cooperation, the correlated pattern frequently narrows the access to one individual well enough to support a subpoena or a deposition, and we state the confidence level plainly.

How long do cloud audit logs last before the evidence is gone?

It depends on the platform and the licensing tier, and the windows are shorter than most executives assume. Microsoft documents the default retention for its Purview audit log by license level, and Google Workspace follows its own schedule for each audit source. Firewall, VPN and endpoint logs are governed by local storage settings and often roll over in weeks. The first preservation task in every engagement is to export these records before the window closes, which is why the call to counsel and to an examiner should come the same day the suspicion arises.

Does the DTSA require us to show the thief actually used our data?

Use is one route among several. Misappropriation under the statute includes acquisition by improper means as well as disclosure or use, so showing that a protected file was taken through theft, breach of a confidentiality duty or electronic espionage can support liability and injunctive relief on its own. Use and disclosure matter a great deal for damages and for the scope of an injunction, which is why the examination documents both the taking and any downstream movement it can find. Counsel decide which theory to plead. We make sure the record for each theory is preserved and analyzed.

What drives the cost of a forensic examination in a trade secret matter?

The number of custodians and devices, the number of cloud tenants and log sources, how much time has passed since the events, whether anti forensic activity has to be reconstructed, and whether the work needs to reach a declaration on an emergency timetable or a full expert report. A focused examination of one departing employee's laptop and cloud account is a very different scope from a multi custodian espionage matter spanning years. We define the scope and the phases in writing after the free initial consultation so counsel can budget each step.

Web Addresses for the Sources Cited

1. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response: https://csrc.nist.gov/pubs/sp/800/86/final
2. 18 U.S.C. 1839: https://www.law.cornell.edu/uscode/text/18/1839
3. Section 1836(b)(2): https://www.law.cornell.edu/uscode/text/18/1836
4. The New York Times on the St. Louis Cardinals and Houston Astros database intrusion, June 16, 2015: https://www.nytimes.com/2015/06/17/sports/baseball/st-louis-cardinals-hack-astros-fbi.html?_r=1
5. Sports Illustrated on the same case, June 18, 2015: https://www.si.com/mlb/2015/06/18/jeff-luhnow-cardinals-astros-hacking-scandal
6. Microsoft Learn, Manage audit log retention policies: https://learn.microsoft.com/en-us/purview/audit-log-retention-policies

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 2026.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.