VESTIGE
Digital Investigations

Non-Compete | IP Theft

Vestige **IP Theft** Services

Our IP Theft Services are a combination of Investigating, Consulting and Testifying Expert services, performed by the Electronic Evidence Experts at Vestige upon the relevant corporate electronic devices to permit a client to rapidly assess and interdict, react, and/or prove unauthorized access, copying, removal, transfer or use of intellectual property and/or confidential information by current or former employees, officers or directors of an organization.

IP Theft Services are offered to timely satisfy two critical needs:
1) Assess the degree of risk that intellectual property has been compromised
2) Respond to IP misuse, wrongful access, and other improper uses of client intellectual property.

Assess Risk

The most difficult challenge in theft of intellectual property matters is determining whether significant IP has been taken. This is because not every potential risk of IP loss justifies the expense, disruption, and potential damage to relationships that may result from complete theft investigation. Crafting the proper response to a particular set of events demands an early, quick assessment of the potential risk and scope of potential damage.

Response

In many cases, clients know IP has been improperly accessed or copied and need to prove the circumstances in a timely manner to support a wide variety of response options such as termination, temporary restraining order (TRO) or litigation. Vestige's services are designed to address client's assessment and response needs.

IP Theft Case Types

- **Violation of non-compete & non-solicitation agreements**
- **Theft of Intellectual Property**
- **Breach of employment agreement fiduciary duty**
- **Violation of Computer Fraud and Abuse Act**
- **Violation of state laws related to accessing electronic information**
- **Patent Infringement**

IP Theft cases rarely are solved by reviewing content on media, instead the digital footprints that are left behind by the individual(s) involved are crucial. Vestige expertise is in identifying, analyzing and opining on these digital footprints.

Vestige **IP Theft Packages**

Complete Response

Utilized when a complete digital investigation and Vestige's expertise is required throughout litigation. Includes full content and artifact analysis, combined with all affidavits, depositions, trial testimony and other services necessary to assist counsel seeking to use electronic evidence to achieve strategic goals within the matter.

TRO Package

For matters in which relevant sources of electronic evidence must be identified, preserved, and analyzed in an expedited manner; and expert opinion(s) formed and defended in Temporary Restraining Order hearings.

Power Package

This is a comprehensive investigative response. Includes preservation of critical electronic evidence and a complete basic forensic analysis based upon the content and artifacts. Includes verbal results.

Triage Package

A 14-point Evaluation of Critical Risk Markers provides clients with a score that reflects the existence of theft artifacts that are highly correlated with significant intellectual property loss. Based upon this risk assessment, clients can craft a response that reflects the degree and quality of evidence.

OVER

Vestige **IP Theft** Details

	Complete Package	TRO Package	Power Investigation	Triage Package
INVESTMENT	$$$$$	$$$$	$$$	$$
Confidential, un-biased 3rd party neutral investigation	•	•	•	•
Non-intrusive preservation of evidence with limited disruption to client organization. *	•	•	•	•
Processes that meet and often exceed the US Department of Justice's Guidelines for the Search & Seizure of Digital Evidence	•	•	•	•
Chain of custody	•	•	•	•
Authentication of digital evidence ensuring admissibility in court	•	•	•	•
Tie-back of digital evidence to physical asset to remove anticipated legal arguments	•	•	•	•
Secure storage / preservation of evidence and maintaining chain of custody	•	•	•	•
Evaluation of Critical Risk Markers indicating likelihood of alleged activities	•	•	•	•
Client | organization questionnaire specific to the matter	•	•	•	
Initial consultation to understand the specifics of the matter (key players, alleged activities, etc.)	•	•	•	
Inventory of digital intellectual property relevant to matter	•	•	•	
Physical evidence integrity verification	•	•	•	
Identification of External Devices associated with system (flash drives, iPod, iPad, external hard drives, etc.)	•	•	•	
Exposure of documents, files and data that's been copied or moved onto external media and/or portable devices	•	•	•	
Detection of burning CDs / DVDs containing organization's IP	•	•	•	
Identification of e-mail accounts, personal or otherwise, where documents, files and data belonging to organization have been directed	•	•	•	
Evaluation of internet history to determine connections to on-line storage repositories	•	•	•	
Analysis of deleted data to classify and identify clean-up, concealment or general deletion activity	•	•	•	
Identification of connections to other individuals and organizations to determine if there are other suspects or internal leaks that need to be addressed	•	•	•	
Evaluation, detection, identification of wiping and/or anti-forensic tool use designed to thwart a digital forensic examination	•	•	•	
Detection of computer fraud and misuse violations	•	•	•	
Oral consultation and discussion findings	•	•	•	
Expertise of investigator	Director	Sr Analyst	Analyst	Analyst
Turnaround time	10 Business Days	72 Hours	12 Business Days	5 Business Days
Standard business hours support	•	•	•	•
After-hours support	⊙	•	⊙	Not Available
Weekend and holiday support	⊙	•	Not Available	Not Available
Retainer	Required		Required	
Terms	See Note **	Prepay Full	Net 30	Prepay Full
Written preliminary findings	•	•		Not Available
Preparation of Interrogatories	•			Not Available
Assistance with deposition of witnesses and/or parties	•			Not Available
Preparation and attendance at hearing	•	•		Not Available
Affidavit Creation	•			Not Available
Deposition of expert	•			Not Available
Expert report	•			Not Available
Preparation and testimony at trial	•			Not Available
Number of devices included	3	3	1	1
Additional devices	Available, call for pricing			

* In-Lab Preservation. [On-site Preservation additional.]
** Balance Prior to Testimony or Net 30, whichever is less.

• Included in Package
⊙ Available service, price based on client need.

Contact Vestige today to discuss your Digital Forensic needs.

TURNING DIGITAL EVIDENCE INTO INTELLIGENCE™

info@VestigeLtd.com | **800.314.4357** | www.VestigeLtd.com