

Digital Forensics | Spoliation

The following descriptions highlight a variety of matters for which Vestige has been retained that involve alleged spoliation. Each of these cases are real matters that we have worked, but for privacy and confidentiality purposes the relevant information has been sanitized. These cases are not the entire population of cases matching such criteria, but instead represent a wide sample of the cases we have worked in this specific area. Should you need additional information, please contact us.

Large Car Dealer v Car Manufacturer | Bad Forensic Images

Vestige represented a large auto dealership (Plaintiff) against a car manufacturer (Defendant). The dealership had an agreement with the manufacturer that the Dealership would always be afforded the same opportunities to open new dealership locations as might be afforded any competing Dealership within a certain radius ("most favored treatment" clause). When the Dealership was not given additional franchise opportunities that were given to competing dealers, the Dealership sued the auto manufacturer for breach of contract. The auto manufacturer fiercely fought discovery. Vestige assisted outside counsel to the Dealership to obtain possession of forensic copies of the computers used by key players to negotiate the contract terms of the agreement with the Dealership. From these forensic images, Vestige extracted all communications and documents related to the Plaintiff's dealership. Vestige also ran its standard verification inquiry over the forensic copies and determined that several of the copies were not complete. These incomplete forensic images were from a computer of a key player. Upon additional examination of the forensic copies, Vestige was able to prove that the copies supplied by the auto manufacturer were of hard drives that had been replaced on the key players' computers during the pendency of litigation and in contravention of a protective order. Additionally, Vestige's analysis of artifacts, residing in special folders accessed by the operating system, proved that data had been erased and the forensic images had been manipulated to hinder analysis. In accordance with the provisions of a protective order, Vestige properly notified the parties and defended its analysis when challenged by the auto manufacturer. The case settled on the eve of trial in a manner that was acceptable to our client.



Chemical Manufacturer v Employee | Undercover Competitor

A manufacturer of a patented chemical discovered that their Vice President of Sales was simultaneously working for a competitor. The manufacturer (Plaintiff) filed a temporary restraining order for violation of a non-compete agreement. The Defendant was pro se (representation without a lawyer) and his defense to the court order, demanding a forensic examination was that he "routinely used information scrubbing software" to protect private and confidential information, including the manufacturer's own proprietary information. The Defendant claimed that he had in fact installed these processes years before the present litigation. Oddly enough, the Defendant simply failed to attend hearings or the trial and received default judgment in the home state of the manufacturer. In an attempt to circumvent the default judgment, the Defendant filed bankruptcy in his state of residency. Throughout a one year process, the manufacturer chased the Defendant in bankruptcy court and finally got an order to conduct a forensic examination on his computer. Vestige discovered that the Defendant had not only failed to stop the destruction process, but instead had installed the disk scrubbing software the afternoon that the judge ordered the turnover of the computer. This was contrary to his original claim that the software was being used routinely before any of the litigation matters became apparent. The end result was a \$400,000 judgment non-dischargeable debt in bankruptcy court in favor of Vestige's client.

Vestige Digital Investigations

TURNING DIGITAL EVIDENCE INTO INTELLIGENCE™

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

Mortgage Company v Individual | IP Theft

Vestige represented a mid-size mortgage company (Plaintiff) against an individual (Defendant) accused of IP theft. The individual was running a branch office in another state for the Plaintiff. During this time, the individual conspired to join a competing mortgage company. Armed with a plan, this individual began stealing client lists and proprietary information from the Plaintiff's company. After the material was taken, the individual would then delete the data off the Plaintiff's server. Most of the information was being taken through the exchange of e-mail between the individual's corporate account and a personal Yahoo! account. Vestige analyzed the branch office computers and the individual's home computer. Vestige discovered that the individual had installed an application called "Window Washer." The individual claimed that the application was used to improve performance, which was in contrast to its obvious function for data wiping. Vestige provided expert testimony during both the preliminary injunction and motion for contempt hearing. Vestige was able to pinpoint when the individual had used the program and that the individual had changed the default settings in Window Washer to achieve a deeper cleanse, such as selectively erasing certain files and activating the automatically clean setting. Despite the individual's attempt to erase data, Vestige still managed to find artifacts left behind by the application. Vestige's client, the Plaintiff, was granted preliminary injunction.



Individual v Mid-size Company | Wrongful Termination

Vestige represented an individual (Plaintiff) against a mid-size company (Defendant) involving a wrongful employment termination matter. Vestige was hired to prove or disprove that the Defendant was thorough in its response to discovery requests from the Plaintiff. Vestige found that the Defendant was not thorough enough in its discovery as information was deleted, new computers were purchased, data was disguised and other storage devices were withheld. Vestige successfully defended its process in multiple hearings and won its client a \$250,000 sanction, and the Defendant's pleadings were stricken as punishment. After a long, drawn-out appeals process, Vestige's client was provided an extremely favorable outcome resulting in an award of over \$11 million dollars in damages and sanctions.



Individual v Large Organization | Anti-Forensic Software

An individual was suing a large organization for wrongful termination and was claiming sexual harassment. The organization believed that some of the evidence that would aid in defending both the wrongful termination and the sexual harassment claims would be residing on the individual's home computer. With the assistance of Vestige, the organization was granted a court order allowing Vestige to conduct analysis of the individual's home computer. Vestige discovered that mass deletion had occurred and that the use of anti-forensic software was implemented to thwart an investigation. Vestige was also able to determine that the anti-forensic software was installed after the court order and was used to delete information pursuant to the litigation at hand. The individual was sanctioned with paying all fees associated with Vestige forensic services and attorney's fees surrounding the motion for spoliation.



Officer v Individual | Fraudulent Evidence - Modified Chat Log

Vestige was hired to examine a paper chat log between an officer (Plaintiff) and a 19 year old individual (Defendant). The Defendant was accused of chatting online with an officer who was acting as a 12-year old girl. The conversations were said to be of inappropriate content and both online parties agreed to meet one another at a mall. The Defendant was subsequently arrested in an area near the mall location, but never actually stopped at the mall. Vestige was hired to examine the paper chat log between the officer and the 19 year old. Vestige proved that the chat log the police officer produced was fraudulent. It was manipulated, changed and edited. Mysteriously, the original computer used by the officer where the chatting occurred was destroyed. The Defendant subsequently won on appeal.



Satellite-Cable Service Provider v Subscriber | Theft

Vestige was involved in a federal district court case for the theft of satellite signals. A satellite-cable service provider claimed that one or more of its subscribers purchased a card writer/reader and, using pirated software, re-programmed a smart card installed in the satellite receiver to permit the subscriber to receive premium channels for free. Vestige was able to assist the cable service provider in obtaining an order permitting access to the subscriber's home computer and thereafter performed a forensic analysis on the computer. Although the subscriber had attempted to hide his pirating activities, Vestige was able to locate and interpret artifacts on the computer that were created by the card reader. Based on Vestige's testimony at trial, a judge held in favor of the cable service provider that the subscriber had re-programmed his satellite receiver smart card. The cable service provider was awarded damages and an injunction against the subscriber.



Regional Retail Entity v Former Franchisee | Trade Dress | IP Theft

Two regional retail entities became involved in a dispute with each other after an accusation of intellectual property theft was made. The IT department of the Plaintiff discovered that a former franchisee (Defendant) had left the Plaintiff's employment to work for its competitor. However, the former franchisee was still accessing proprietary franchisee information from Plaintiff's extranet and passing that information along to the competitor. Vestige was appointed by the court to facilitate the discovery process and investigate computer systems for both sides. Vestige imaged and analyzed approximately 90 computers between the two entities. Vestige's analysis indicated that the Defendant in this matter had spoliated evidence on approximately 25 out of 35 systems in its possession. The revelation of this fact resulted in an expedited settlement in favor of the Plaintiff.



Individual v Individual | Breach of Fiduciary Duty

Vestige represented an individual (Defendant) against another individual (Plaintiff) who filed a lawsuit for breach of fiduciary duty for not attending important business meetings, not involving themselves in business affairs, failing to provide adequate capital and failing to provide an operating plan. The Defendant counterclaimed. Vestige analyzed the Plaintiff's computers for communications and files relevant to the matter. Vestige uncovered that the Plaintiff destroyed information on his computer. More specifically, Vestige was able to prove that the Plaintiff took affirmative actions to destroy a folder that any reasonable person would suspect to contain relevant data. Vestige helped prove the elements of a spoliation claim, which resulted in the Plaintiff's claim being dismissed and the Defendant's counter claim being granted. All costs related to the spoliation were paid by the Plaintiff.



Vestige Digital Investigations

TURNING DIGITAL EVIDENCE INTO INTELLIGENCE™

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