Case Study: Stabilizing an Urgent IP Breach with Defensible Digital Forensics

A long-time client in the medical device industry contacted Avalon with an urgent concern: A current or former employee was suspected of removing confidential design files, engineering documentation, or proprietary process information. With legal timelines moving quickly, the client needed to preserve evidence, prevent spoliation, and support outside counsel with defensible forensic analysis.

They also required a clear, efficient workflow that connected forensic investigation with attorney review of potentially relevant electronically stored information (ESI). Avalon was engaged to act as an extension of their team – providing project management, chain-of-custody rigor, and the ability to translate technical findings into clear legal insights.

The Challenge

The client needed to quickly determine whether sensitive intellectual property (IP) had been accessed, copied, or exfiltrated, and ensure the investigation would withstand legal scrutiny. Potential evidence spanned multiple sources, including workstations, email, collaboration tools, removable media, and possible personal cloud accounts. They required rapid preservation, minimal business disruption, and a seamless path from forensic findings to attorney review – all while maintaining strict confidentiality and evidence integrity.

The client needed to quickly determine whether **sensitive intellectual property (IP) had been accessed, copied, or exfiltrated,** and ensure the investigation would **withstand legal scrutiny.**

The Strategy

Avalon's digital forensics team worked with counsel to define objectives, identify key custodians, prioritize data sources, and align with legal deadlines. We developed a targeted collection plan that preserved the most critical evidence first while maintaining strict chain of custody controls.

Our forensic analysis focused on indicators of IP movement, including USB activity, file access and modification patterns, print logs, external storage usage, and potential transfers through email or third party tools. We examined system artifacts – such as logs, link files, browser history, and cloud sync traces – to establish who did what, when, and how. For mobile and collaboration platforms, we coordinated collections and reviewed relevant messaging and activity.

To support the legal team, we built a streamlined eDiscovery workflow. Relevant ESI was organized into a review ready structure, with

search strategy and culling support to reduce noise and surface key documents quickly. Throughout the engagement, Avalon maintained close communication with the client and counsel to support real-time decision-making.

The Results

Avalon delivered a coordinated, defensible approach that combined digital forensics and eDiscovery under one roof – eliminating the need for multiple vendors during a high pressure investigation. Our targeted collections and deep forensic analysis – including deleted data, system artifacts, and cloud activity – preserved evidence integrity and accelerated fact development.

By providing structured reporting and a review ready Relativity workspace, we enabled counsel to identify critical documents early and move quickly on strategic decisions. The client gained rapid clarity into what occurred, preserved essential data sources, and established a defensible foundation for next steps. Finally, the integrated workflow kept momentum strong during a sensitive and time critical matter.

QUESTIONS?

For more information on any of our services, please contact: