



Remote Digital Forensics, eDiscovery
and Investigations

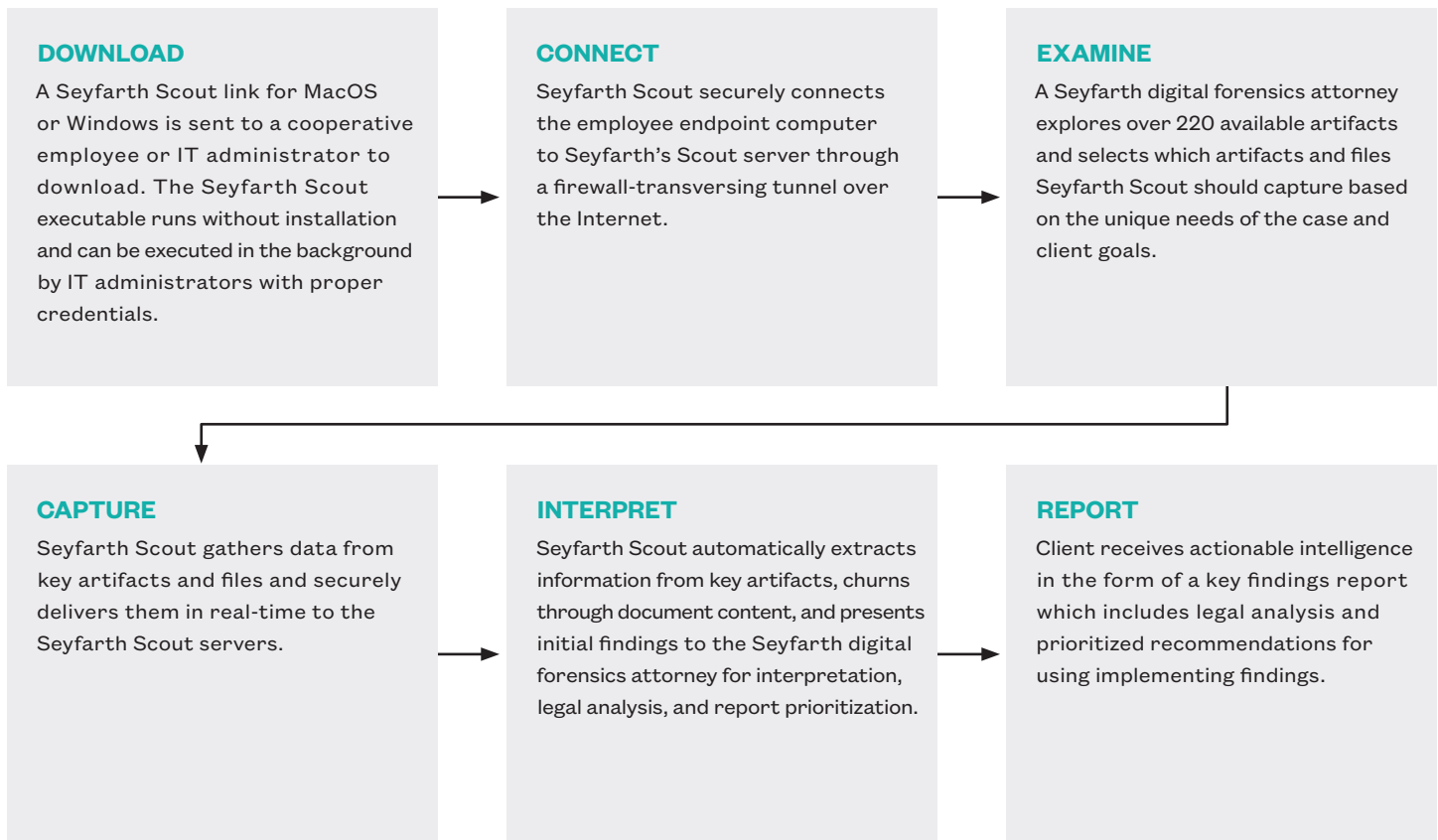
The COVID-19 pandemic has forced millions of employees to work from home, which creates an inherent risk for businesses of all types. Prior to the pandemic, we had begun developing Seyfarth Scout—a one-click application service to remotely conduct digital forensic triage, employee investigations, and eDiscovery preservation of remote computers via the internet. Using this proprietary tool, what used to take days now takes only a few hours, providing clients with early information that could critically change the course of your response and inform your strategy.

Seyfarth Scout is a forensic software workflow that collects data for high-priority triage, including usage of USB devices, internet history, mass deletions, cloud/sharing service access, file access, and more than 220 other data points. For a predictable flat fee, Seyfarth Scout focuses on the most critical and relevant data artifacts while avoiding the need to capture a full forensic image. This avoids on-site forensic consultant visits or shipping hardware back and forth through common carrier. Ultimately, Seyfarth Scout significantly reduces costs and time.

Why Seyfarth Scout?

- Remotely targets, collects, analyzes, and reports more than 220 key data artifacts from remote computers for early case assessment and zero-day evidence collection.
- Provides actionable intelligence to inform clients of critical information earlier in a matter lifecycle.
- Background installation and execution with IT application push capability or remote administrator credentials. Also includes a one-click custodian user executable for cooperative targets.
- Seyfarth Scout can also retrieve data from over 50 of the most popular cloud services.
- Works with both Windows and MacOS target endpoints.
- End-to-end encrypted transport with full firewall transversal to securely transfer data while avoiding connection issues.
- Features a keep-alive system to ensure automatic resuming of data collection if a target goes offline for a period of time.
- Includes privileged reporting, interpretation, and legal-focused strategy recommendations.
- Quick turnaround time avoids waiting days for results through traditional means.
- Social media and website membership discovery from over 350 known websites.
- Ideal use cases:
 - Employee investigations
 - Trade secret misappropriation investigations
 - Legal hold preservation / eDiscovery collection
 - Privacy, compliance, and records retention

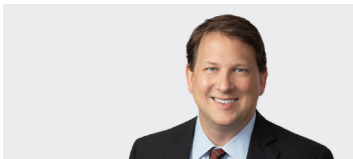
How Seyfarth Scout Works



eDiscovery Preservation

In addition to its investigational uses, Seyfarth Scout is also able to conduct rapid data identification and collection to help clients comply with legal hold obligations. Leveraging the secure remote connection capability, Seyfarth Scout can quickly report on computer hard drive contents and assist with capturing and preserving potentially relevant data into forensic evidence containers. Because Seyfarth certified digital forensic attorneys carry out the procedure, the process is privileged, avoiding discovery about discovery from aggressive opposing parties.

Key Contact:



Jay Carle

Chicago
(312) 460-6426
jcarle@seyfarth.com