CRIMSON VISTA

Digital Forensics & Investigations

When a breach or suspicious event occurs, you need answers—fast. And the accuracy of the facts matter. Crimson Vista's Forensics & Investigations team uncovers what happened, how, and why. We deliver actionable evidence you can trust. Our experts go beyond detection to provide attribution, legal defensibility, and closure. Our Digital Forensics & Investigations Services include:

DataVeracity℠ Data Forensics & Breach Analysis

Data is the life-blood of your company. If you know, or even suspect, that something might be wrong with your data, DataVeracity℠ can help. Our DataVeracity℠ service captures forensic images, analyzes them for data of interest, and can even reveal some amount of lost or deleted data. Moreover, our analysts can dig into the bread-crumb trails of devices, systems, and logs to find out how the data got into its present state.

- Forensic imaging of data sources
- Log-file analysis
- Metadata analysis
- Data Recovery
- Attribution and timeline

Traceback℠ Source Code Forensics

Understanding source code is hard. The truth is, even most software engineers do not fully understand the systems they create, let alone third-party libraries and other software supply-chain components. This makes it challenging when an unexpected incident demands knowledge of how the source code operates. Traceback℠ is Crimson Vista's service for rapid code comprehension both statically and over time. We help engineers, legal teams, and auditors understand the operations, algorithms, and data structures in their organization's source code. We can also analyze the development history to reveal when features or bugs were introduced, who introduced them, and their evolution from introduction to the present. Whether to prove IP theft or explain how an intrusion occurred, Traceback℠ provides clarity and insight.

- IP theft, malicious logic, or hidden vulnerabilities
- Attribution and attestation
- Cross-references with technical documentation and other engineering artifacts
- Specialized knowledge in advanced areas such as AI, ML, cryptography, and wireless communications
- eDiscovery

Private Eye℠ Custom Technical Investigations

Digital incidents are, in modern systems, potentially world-wide affairs. Data may be in data stores around the world, as are the vendors, the customers, and the regulators. From insider threats to policy violations, Eye℠ tackles the unexpected. If it touches tech and needs a closer look, we investigate it—quietly, thoroughly, and professionally.

As a testament to our continued commitment to excellence in cybersecurity, a comprehensive list of our Team's professional certifications can be found on our website in the Collective Knowledge section.

- Cryptocurrency tracing (Chainalysis certified)
- Insider access, theft, and manipulation
- Post-breach analysis of handling and response
- Standard of care considerations and analysis
- Reverse Engineering
- Password Cracking
- eDiscovery

ABOUT CRIMSON VISTA

Our Advanced Persistent Defense (APD) approach is central to how we protect our clients. Cyber threats aren't one-off events—they're ongoing, evolving risks. APD emphasizes continuous monitoring, rapid response, and proactive adaptation to ensure you're not just reacting to threats but staying ahead of them. By layering proactive defense measures with intelligent risk detection, we provide round-the-clock protection against even the most sophisticated attacks.