



MARK CLEWS

Managing Director



Mr. Clews is a Digital Forensics and eDiscovery expert with over 20 years of experience advising clients on managing electronically stored evidence. He specializes in preserving and analyzing digital evidence, handling complex data, and leading large-scale discovery matters.

He has experience across the full EDRM lifecycle, from information governance and readiness through data preservation, processing, and review. He has led hundreds of engagements, ranging from single-device forensics to multi-jurisdictional class actions.

Mr. Clews has supported clients in regulatory investigations involving agencies such as the SEC, DOJ, FTC, and others, and has worked on matters including intellectual property theft, fraud, and cartel investigations.

He has earned multiple forensic certifications (MCFE, EnCE, CCFP) and has been recognized globally as a leading expert in digital forensics and eDiscovery.

Most recently, he built and launched a digital forensics service line at a global consultancy, developing operational workflows, publishing thought leadership, and establishing secure evidence management processes and facilities.

iDiscovery Solutions, Inc.
535 Anton Blvd., Suite 860
Costa Mesa, CA 92626

+1.949.231.0473

mclews@idsinc.com

 [Profile on LinkedIn](#)

 [@iDiscoveryInc](#)



EDUCATION

- BPP Business School, London, Certified Accounting Technician (CAT)

EXPERIENCE

- iDiscovery Solutions; Managing Director; April 2026 to present
- Vertex Companies LLC, Director; July 2025 to December 2025
- Ankura Consulting, Senior Managing Director; August 2018 to December 2024
- Navigant Consulting, Managing Director; June 2006 to August 2018
- BDO LLP, Senior Forensics Accountant; March 1998 to June 2006

PROFESSIONAL EXPERIENCE

- Mr. Clews was retained by a health insurance company as the digital forensic expert to assist in their response to the National Association of Insurance Carriers (NAIC) after a suspected data breach. Mr. Clews was tasked with interviewing data stewards within the company and identifying potential sources of evidence. Once identified, Mr. Clews and his team preserved all the potentially relevant data sources in a defensible manner. Data for over 70 custodians was successfully preserved. Data sources included Laptops, Email, Instant Messages, removable drives, network collections, websites, blogs, social media accounts and virtual machines.
- Mr. Clews was retained by a health care provider to assist them respond to a whistleblower lawsuit. He was tasked in overseeing the defensible collection of over 300 electronic devices totaling ~50 terabytes of data. Devices in scope included desktops, laptops, local email, cloud-based file repositories, cloud-based email, removable drives, server shares, mobile devices and accounting systems. Once the data had been successfully preserved, Mr. Clews managed the identification, extraction, data processing, review and production of the potentially relevant data. He worked closely with Ankura's custom application team to develop a custom solution to achieve efficient review of mobile device artifacts leveraging multiple reviewers.
- Mr. Clews was appointed the Independent Forensic Expert in a Financial Industry Regulatory Authority (FINRA) Arbitration. He was tasked with auditing a telecommunications company's identification and preservation processes, which were ultimately deemed insufficient. Mr. Clews managed the restoration of backup tapes from the time of the original collection and ran search terms across the data to identify responsive documents. He then used forensic techniques to remove duplicates and create a differential delivery to the other parties in both Concordance and Summation formats. His assistance on this matter led to a substantially larger document set being identified for disclosure.



- Mr. Clews was appointed as the digital forensic expert in a theft of intellectual property case on behalf of a television network. Mark was tasked with reviewing the opposing side's forensic expert's methodology and observations. Mark was able to successfully challenge the contents of his report, resulting in the judge agreeing to all of the plaintiff's requests and ultimately led to an out of court settlement.
- Mr. Clews was appointed as the forensic expert to assist a social media company respond to a Securities and Exchange Commission (SEC) investigation relating to their initial public offering (IPO). Mark managed the forensically sound collection and analysis of over 100 digital devices including laptops, desktops, tablets and mobile devices. During the case, Mr. Clews successfully audited the performance of two email archiving tools, Enterprise Vault and Proofpoint.
- Mr. Clews was appointed as a forensic expert to investigate allegations of theft of intellectual property from an auto-financing company. Mark was able to rebuild the timeline and reconcile user activity from the clients CRM system and the custodian's laptop. Mark was able to locate evidence artifacts that indicated that the custodian had downloaded customer lists prior to leaving employment. Using forensic techniques, Mark was able to identify a USB device which had been used to exfiltrate the intellectual property outside the enterprise.
- Mark investigated a large Internet Service Provider (ISP) for accounting irregularities on behalf of the Securities and Exchange Commission (SEC). He led the Computer Forensics team in analyzing all electronic evidence to identify potentially relevant data. He established a workflow using Guidance Software's EnCase to filter out system file types and known files based on a comparison of the NSRL's known hash database. He also oversaw the subsequent loading of these files into a platform for attorney review. Mark's work on this project assisted the SEC in reaching a \$300 million penalty settlement with the ISP.
- Mark assisted a Fortune 500 corporation in their response to a European Union Competition Commission investigation into cartel practices. He led a team in the collection of hundreds of custodian laptops, user share areas and departmental shares. The data resided across numerous sites and countries and considerations had to be taken in relation to jurisdictional data protection laws. He successfully developed a methodology to access the collected data circumventing 'SafeGuard Easy' full disk encryption and managed the deliveries to the third party review platform.
- Mark conducted a forensic investigation on behalf of a recruitment consulting firm in relation to allegations of theft of intellectual property. He analyzed the suspect's computer and successfully identified forensic artifacts which suggested a removable device was used to copy the firms' prospective candidate database. This led to his client successfully obtaining a cease and desist order.



TESTIMONY EXPERIENCE

- July, 12 2025; All Pro Communication Technologies, Inc vs. Hrach Rostami, Et Al., Los Angeles County Superior Courts, West Covina, Trial Testimony.
- January, 22 2024, First Team Real Estate – Orange County vs. Lewandowski, Superior Court of California, County of Orange, Trial Testimony.

CERTIFICATIONS

- Magnet Certified Forensic Examiner (MCFE)
- EnCase Certified Examiner (EnCE)
- Certified Cyber Forensic Professional (CCFP)

PUBLICATIONS

- Protecting Trade Secrets is the New Normal, May 2020
- UV Lights, Mud Balls, and the Courtroom: What TaylorMade v. Callaway Means for Sports Litigation, April 2026

