

Criminal Defense and Litigation Counsel Response to Oxygen Forensics, Inc. Foreign Ownership: Investigating Lab Certification and Examiner Validation Methodology

Legal Opinion | September 24, 2026

As stated in a [Press Release from the U.S. Attorney's Office](#), Central District of California, dated September 23, 2026, the United States Department of Justice announced the arrest of the CEO of Oxygen Forensics, Inc pursuant to a criminal complaint filed in the U.S. District Court, Central District of California, Case No. 2:26-mj-054999-DUTY alleging Conspiracy to Commit Wire Fraud in violation of U.S. Code Title 18, Section 1349.

The Oxygen Forensics software is used to recover, preserve, and analyze electronic data from digital devices while keeping the original files unchanged. According to the Press Release, officers of Oxygen Forensics, Inc. fraudulently represented to the U.S. government that Oxygen Forensics had no immediate or highest-level Russian owner and concealed that the Oxygen Forensics software was developed in Russia.

These fraudulent representations, among other actions, were undertaken to make it appear that Oxygen Forensics was eligible to sell its software to government agencies, and to cause those agencies to rely upon fraudulent representations. The agencies that so relied included U.S. Secret Service, National Computer Forensics Institute, Homeland Security Investigations, and the DHS Office of Inspector General. While the criminal complaint focuses upon the representations made, the complaint does not allege that the Oxygen Forensics software contains malicious code or was used to gain unauthorized access to any customer computer system or data.

The disclosure in the Press Release is that Oxygen Forensics, as a supply chain provider of forensic software, lied to various government agencies. This author suggests that the criminal complaint in this matter provides sufficient ground upon which civil litigators and criminal defense attorneys ought to identify for each of their e-discovery vendors or digital forensic examiners the manner in which each has discharged due diligence obligations to vetted ownership of forensic tool suppliers as part of certification protocols or as part of their reliability validation framework.

Due diligence obligations related to supplier ownership and supply chain cybersecurity risk mitigation

NIST SP 800-161 Rev. 1 sets forth guidance to manage cybersecurity risks in supply chain purchases. The standard expressly supports best practices including ownership inquiries related to supply chain suppliers at all levels of an organization. The November 2024 update to SP 800-161 Revision 1 includes questions about verification of supplier ownership and foreign ownership, control, or influence, and presents those questions in a template to be tailored to the organization and selected controls. ([NIST SP 800-161 Rev. 1 Update 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, Appendix D, §§ D.4, D.4.1.3, pp. 217, 221.](#)) NIST's supplier due-diligence guidance also applies to suppliers of products when purchasing or acquiring new systems, including information and communication systems. ([NIST SP 1326, Due Diligence Assessment Quick-Start Guide \(July 2026\), pp. 2, 15.](#)) NIST's July 2026 guide asks, "Does this company have foreign ownership, investment, or headquarters?" and addresses foreign-government ties and laws requiring cooperation with foreign security services. ([NIST SP 1326, p. 8.](#)) Its provenance review also addresses development locations and the locations of key source-code developers. ([NIST SP 1326, p. 9.](#))

The author suggests that while it is prudent that digital forensic entities and individual digital forensic examiners mitigate supply chain cybersecurity risk by compliance with this NIST standard, the Oxygen Forensics criminal complaint focuses attorneys upon this risk as a reliability issues. The author suggests that all digital forensic entities and individual digital forensic examiners ought to mitigate supply chain cybersecurity risk by compliance with this NIST standard and anticipate inquiries from clients regarding internal mitigation processes implemented.

Some digital forensic entities provide additional measures of credibility by providing laboratory certifications. Relevant Laboratory standards also may provide require due diligence related to forensic tool supplier review. For example, ISO/IEC 17025:2017 (General Requirements for the competence of testing and calibration laboratories) requires a laboratory subject to the standard to establish procedures and retain records for evaluating, selecting, monitoring, and reevaluating external providers, and for taking action arising from those reviews. ([ISO/IEC 17025:2017, § 6.6.2\(a\)–\(d\), p. 9, public reproduction.](#)) While these standards do not expressly require an investigation of foreign ownership, NIST's crosswalk confirms the standard's supplier-evaluation and reevaluation requirements. ([ISO/IEC 17025:2017, §§ 6.6.1–6.6.2, pp. 8–9, NIST, ISO/IEC 17025 Crosswalk: Supplies and Supplier Evaluation \(March 2018\), pp. 1–2.](#))

Due diligence obligations related to Expert Testimony reliability.

When seeking to admit digital forensic expert testimony, Criminal defense counsel and/or Civil litigators can examine the facts, methods, and assumptions supporting an expert's opinion, including the underlying facts or data on cross examination. See [Fed. R. Evid. 705](#). Additionally, counsel can probe the reliability of

the application of digital forensic tools to the facts and/or analysis underlying expert testimony. See Fed. R. Evid. 702. Federal Rule of Evidence 702 places the admissibility burden on the proponent, who must establish, more likely than not, the rule's requirements concerning supporting data, reliable methods, and reliable application to the facts of the case. (Fed. R. Evid. 702(b)-(d).)

The Scientific Working Group on Digital Evidence recommends an isolated, secure, known examination environment and forensic tools that are updated, tested, and validated before examinations (Scientific Working Group on Digital Evidence, Best Practices for Computer Forensic Examinations, 18-F-001-2.0 (July 28, 2025), §§ 4.2-4.2.2. and Scientific Working Group on Digital Evidence, 20-F-005-2.0 (June 23, 2026), related to mobile devices,

The author is of the opinion that the guidelines set forth by the Scientific Working Group on Digital Evidence for both computers (SWGDE 18-F-001-2.0, §§ 4.2-4.2.2) and cell phones (SWGDE 20-F-005-2.0) ought to be an integral part of the methodology used by digital forensic examiners to validate forensic tools they purchase from supply chain providers. Prudent digital forensic examiners ought to anticipate that knowledgeable attorneys during cross examination will likely probe the examiner's competence by including questions about the examiner's method of reviewing and evaluating forensic tool supplies.

1. "What responsibilities did you have for selecting the software or evaluating its supplier?"
2. "Who was responsible for that review, and what policy governed it?"
3. "What vendor representations, if any, did you rely on when assessing the software's development or security controls?"
4. "Did those representations affect the decision to use the product or the checks you performed?"

The author is of the opinion that the Oxygen Forensics disclosures in the Press Release provide civil and criminal defense attorneys with a foundation to explore the methods used by digital forensic entities and experts to choose the software tools they use. Such a review policy is best described as an integral part of the validation and reliability requirements of expert witness testimony, and is an integral part of the cybersecurity risk management needed in the modern world. Whether such an inquiry is frustrated by law enforcement's claim of privilege is a topic for a future blog.

About the Author

Donald Wochna

Highly accomplished attorney with 41 years of legal practice, uniquely certified as a Computer/Cell Phone Forensic Expert (CCFE, CMFE) and seasoned litigator. Specializes in computer forensics, mobile device forensics, e-discovery, cybersecurity, and data privacy, serving as a consulting and testifying expert witness. Leverages deep expertise in investigative frameworks and electronic evidence integration to translate complex technological and legal concepts for diverse audiences, empowering clients to effectively address emerging data and electronic device challenges.