Technology,
Civil Litigation
Dec. 10, 2021

Bookmark

5 commandments for selecting a digital forensic expert

DANIEL B. GARRIE
Neutral, JAMS

Cyber Security

Cell: (212) 826-5351

Email: daniel@lawandforensics.com

Daniel is an arbitrator, forensic neutral and technical special master at JAMS, available in Los Angeles, New York and Seattle. He is co-founder of Law & Forensics LLC, and head of its computer forensics and cybersecurity practice groups, with locations in the United States, Europe, and Israel. Daniel has authored over 200 legal and technical publications and his scholarship has been cited in over 500 articles, publications, and cases.

See more...

GAIL A. ANDLER
Neutral, JAMS

Email: gandler@jamsadr.com

Gail A. Andler is a retired judge of the Orange County Superior Court. She is a Southern California-based neutral who specializes in business, employment, class actions, and mass torts.

See more...

BRADFORD K. NEWMAN
Partner, Baker & McKenzie LLP

Email:
Bradford.Newman@bakermckenzie.com

See more...

Litigators and judges increasingly are being asked to weigh and assess what computer forensic evidence purports to demonstrate in varied -- and often contested -- scenarios. So, the services of digital forensic experts and their reports in a litigation cycle are not only in greater demand today, but often can dictate the outcome of serious disputes. The market is crowded, and the search to engage these experts can be complicated and time-consuming. The following commandments will guide litigators and clients on the work of digital forensic experts and critical factors that should be considered when selecting one.

1. Trust but verify the digital forensic expert's specific and related experience

Like the law itself, digital forensics has many nuances, so selecting a digital forensic expert requires you to evaluate the specific and related experience. When evaluating a digital forensic expert's qualifications, the expert must explain their particular technical experience as related to the case. They should provide any filed reports, subject to confidentiality. Litigators should inquire as to what technical certifications related to computer repair, networking, or any other relevant information technology disciplines and digital certifications the expert may have, as technical certifications are different from digital forensic certifications. Unlike technical certifications, many forensic certifications can be procured simply by paying a fee to the sponsoring organization and completing the most basic requirements. Certifications specific to digital forensics can indicate the level of an expert's competency, but it is their technical computer science certifications that reveal the true level of expertise. This will help to determine the likelihood that the expert will be able to adequately qualify in court as an expert and effectively rebut efforts by the other side to confuse or distort the evidence.

The digital forensic expert will often not have the exact experience, but it is important to ensure that the expert's related experience is relevant to the client's needs in the particular case. For example, the case may include multiple types of evidence, such as computers, mobile phones and social media accounts. It is critical that the selected expert have experience in these areas. If the expert is relying on a team, understand what work will be delegated, and the background and experience of the members of the team. Also, it is important to look for prior deposition transcripts for the expert so you will know not only how they have described their experience and qualifications but how they have been cross-examined about the imits of their experience, as well as their opinions.

2. Make sure the digital forensic expert report is based on 1s and 0s.

A digital forensic expert report is often compiled at some point during the engagement. It is imperative that the report is a technical and scientific document without legal argument. The report's focus must be on thethe facts uncovered, and logical conclusions that can be drawn from the 1s and 0s. Itt should also summarize the process and findings of the digital forensic engagement, meaning another digital forensic expert can use the report and evidence analyzed to replicate the conclusion in the report. When this is achieved, it indicates that the digital forensic expert did a good job because the report can stand on its own without any additional context from the digital forensic expert.

3. Do not confuse an ediscovery expert with a digital forensic expert.

This is the most common mistake litigators make, and understandable since ediscovery and digital forensics are somewhat similar in nature. However, the critical differences center around how the data is collected and presented, how it is reviewed and interpreted, how much data is involved, and whether professionals are required to engage in forensic data recovery. Ediscovery does not analyze or investigate data and its uses. It helps to gather and organize information and large data sets that can be viewed, accessed, duplicated and ultimately produced to the opposing party. The focus of digital forensics is distinct. If someone (usually a malicious actor like a former employee) deletes or steals data, a digital forensic specialist can often use tools and training to detect what occurred, and potentially aid the parties or the court in recovering or retrieving it. In this case of an employee deleting or stealing data, a digital forensic expert will need to determine if the intentional destruction claim is true and how the user destroyed the data. In sum, digital forensic experts deterine what happened and use forensically sound tecniques to gather, preserve and restore data, while ediscovery processes and delivers the data to the appropriate parties. One must be careful to select a litigation support company that has the needed experience in these two disciplines.

4. Just the facts -- legal conclusions should not be a part of the expert report.

In the final stages of a digital forensic expert's work, she will often create a professional report to document all relevant findings of the investigations. This report will describe the activities undertaken during the investigation, a timeline that correlated evidence with user activities, the digital forensic expert's opinions based on her experience and qualifications, and her conclusions based on the evidence. A digital forensic expert must not include legal conclusions in her report, norcomment on the guilt or innocence of an involved party. Her report should only be premised on the facts of the investigation. All expert reports of the investigation should be prepared with the understanding that they will be heavilyscrutinized by the opposing party and experts, as well as by the court. Legal conclusions are solely for the court to make, and ultimate determinations of civl liability or criminal guilt are exclusively made by the finder of fact. The most effective digital forensic experts explain the evidence in a manner designed to educate the court and/or jury as to why the "0s and 1s" mot likely mean X did -- or did -- not occur.

5. Ensure that the chain of custody is complete and accurate.

The chain of custody demonstrates trust to the courts and the clients that the evidence has not been tampered. It is the most critical process in evidence documentation. Each step in the chain is important because if broken, the evidence may be rendered inadmissible. The chain of custody assures the court of law that the evidence is authentic. It shows the court that the evidence was in the custody of a person designated to handle it at all times, and it was never unaccounted. Despite this process being lengthy, it is essential for evidence to be deemed admissible and relevant in the court of law.

While the abovementioned commandments are essential for all litigators, it is clear that lawyers need to understand technology. If lawyers do not understand the basics around the technology used by the custodians at issue and the way forensics work across different medias, they will not be able to effectively guide and work with the digital forensic expert, and understand her findings. They will also struggle to persuade the opposing counsel, court or jury. .

Although not every dispute or litigation matter will involve large sets of data, it is highly possible that one will find some computerized device or data, such as a web search, single text message, email, voice mail, transaction record, or the like. As electronically stored information becomes more dominant, so too does choosing the right digital forensic expert. In fact, the outcome for your client may depend on it. □

#365298