How to Find a Digital Forensics Expert

John Edwards - Law Technology News

11-29-2012

Whether searching for evidence in a criminal prosecution or determining employee activities in a civil dispute, lawyers are increasingly calling on digital forensics experts for investigatory and expert testimony services.

Digital forensics specialists possess unique talents that distinguish them from other tech experts. "Founded in law enforcement, digital forensics encompasses legal, technical, and investigative knowledge," observed Alton Sizemore, a former FBI special agent who managed programs in cybercrime and white-collar crime. "A major differentiator between digital forensics and IT is the forensic expert's training and experience in the preservation and analysis of digital evidence and the ability to present their findings in a court of law," said Sizemore, who is currently director of investigations at Forensic Strategic Solutions, a forensics investigation firm headquartered in Birmingham, Ala.

GETTING STARTED

Like many other types of expert consultants, digital forensics specialists are frequently found by word of mouth. "Attorneys seeking a digital forensics expert will many times send an intra-office email asking if other attorneys in the firm have had good results with particular expert," said Donald Wochna, chief legal officer at Vestige Digital Investigations, a computer forensics firm located in Medina, Ohio. Wochna added that many digital forensic experts enjoy excellent reputations from testifying in court, authoring books, and providing presentations and seminars.

"Most of my clients come to me by referrals," said Vinny Troia, a digital forensics investigator at Night Lion Security, an IT security company with offices in New York, St. Louis, and Washington, D.C. "Almost all attorneys know some IT people; sometimes, it's just a matter of connecting the dots."

Sizemore recommended hiring an expert as soon as the need arises. "Because digital evidence is easily compromised, hiring an expert early in the litigation process can help ensure that valuable evidence is preserved," he said. "Moreover, the proper analysis and interpretation of digital evidence not only takes time, but can be the difference between winning and losing your case."

Steven Gill, a managing partner at BTB Security, an IT security and forensics firm located near Philadelphia, said that a digital forensics expert should have strong investigatory skills, data and image acquisition skills, and an ability to create and maintain detailed documentation. The expert should also have keep knowledge of relevant computer and mobile device platforms, such as Microsoft Windows, Linux, Apple IOS, and Google Android, as well as experience with investigatory tools like Guidance Software's EnCase Forensic and FTK's Forensic Toolkit. "It's important to verify all of these [skills]," Gill said. "For example, you may find a very competent forensic examiner; it just might not be the right case for his or her first time reviewing a Mac-based system."

Lawyers should also look for digital forensics experts with strong e-discovery process knowledge and abilities. "I would also highly recommend querying the candidate on their experience with managing a chain of custody process for criminal cases specifically and request sample report deliverables to verify the quality of the expert's work," said Anthony Williams, a security and forensics instructor at TrainACE, a Greenbelt, Md.-based computer and security training company.

QUALIFICATIONS AND QUALITY

Certification provides evidence that a digital forensics expert possesses basic knowledge of generally accepted forensics procedures and practices. "There are several computer and digital forensics certifications that a lawyer could look for, such as a CHFI (Computer Hacking Forensic Investigator), CCFE (Certified Computer Forensics Examiner) or the DFCB (Digital Forensic Certification Board)," Williams said. "Anyone holding one or more of these certifications has been trained in digital forensics process and has also had some exposure to preparation as an expert witness."

Prior experience as an expert witness is a useful, but not necessarily an essential attribute in a digital forensics specialist. "There's a first time for everything, including expert witness testimony," Gill said. "If the person is competent, articulate, and possesses the skills required to translate difficult technical jargon to layman's terms, previous experience as an expert witness might not be necessary."

To spot unqualified candidates, Damon Petraglia, forensic and information security services director at Chartstone Consulting, a digital forensic service provider headquartered in Fairfield County, Conn., suggested asking a series of case-relevant questions. "These questions should have elements of criminal or civil procedure, rules of evidence, investigative techniques and relevant technological protocols," he said. "The qualified expert will be able to blend these topics to create a holistic investigative view and create a plan, procedure and tool selection to address the needs of the particular case."

In the interview with a candidate, said Petraglia, "it would be good to provide a hypothetical scenario where some type of valued data were stolen from a computer or network." In building the hypothetical, consider whether "email and several network protocols for data transfer have been ruled out as potential avenues of exfiltration," continued Petraglia." Have the candidate identify alternate methods of exfiltration and incorporate a process to investigate. The candidate should identify removable media, including USB devices as a method of exfiltration. The candidate should then walk through the process for this particular scenario."

Wochna said that the most common mistake an unqualified expert makes is testifying beyond the limits of the supporting evidence. Some forensic examiners profess to be image experts, especially in child pornography cases, and may claim expertise not supported by the profession, said Wochna. "Examiners that, for example, profess to be able to discern the identify of the specific person operating a keyboard during a critical time, generally expose themselves to damaging cross-examination in which they must admit that there are no forensic artifacts that identify unique individuals," he explained.

The cost of hiring digital forensic experts vary widely. "I have seen hourly rates as low as $100 per hour to upwards of $600 per hour," Gill said. Location, experience, and the size of the expert's support team all play a role in the determining hourly rates. "Also, some states [such as Calif. and Fla.] require forensic examiners to be licensed and bonded as a private investigator, which can drive up costs," Gill observed.

Wochna suggested looking for a digital forensics expert who has a consistent track record of working closely with attorneys. "The best examiners are those that provide the attorney [with] the good, the bad, and the ugly of a case and allow the attorney to strategically use the expert’s opinion to identify issues associated with the claims, defenses and damages," he said.

Interviewing multiple forensics specialists before making a final decision is always a good idea, advised Gill. "Even though several [experts] may be good, you might find one in particular that works best with your style," he noted. It's also useful to gradually build a portfolio of experts knowledgeable in different forensic areas, Gill said.

Peter Coons, a senior vice president at D4 eDiscovery, a digital forensics company headquartered in Rochester, N.Y., said that forensics expert candidates should be scrutinized as closely and carefully as applicants for a full time job. "Ask for a resume/CV [curriculum vitae] and [then] call references," he said.

"Ask if you can review transcripts of prior testimony both written and oral, give the person a five-minute Q&A session that's like a mock trial — direct and cross — and ask them what they like and dislike about testifying."

Before beginning to look for a forensics expert, Sizemore said that a lawyer should learn as much as possible about the type and scope of digital evidence involved in the pending case. "Not only will your knowledge enable you to narrow your search for a qualified forensics expert, but it will ultimately help you control the cost of the engagement," he said.

John Edwards is a freelance writer based in Arizona. E-mail: jedwards@gojohnedwards.com.