



What to Look for in an Electronic Evidence Discovery Firm

By Monique Mattei Ferraro, JD, CISSP

When diving into unfamiliar waters, it seems reasonable to stick with the life preserver that saved you in the past rather than to reach for a smaller, closer tube that would also carry your weight. Similarly, some law firms are probably overpaying for electronic evidence discovery (EED) services and not getting the most bang for their buck. Many law firms opt for large accounting, audit, or investigative firms because of their familiarity with them and their past relationships. Seems reasonable enough, but it may be cheaper and faster to employ a local, smaller firm.

Here's some guidance on EED, including when to use a larger EED firm versus a smaller firm, what qualifications to look for in an expert, and information about common EED expert certifications.

What Can an EED Expert Help With?

EED refers to all matters related to the discovery of electronic evidence. EED encompasses everything from the humongous e-mail and document discovery in mammoth corporate litigation cases like those involving Enron and Microsoft to obtaining the e-mails from a cheating spouse to her lover in a bitter divorce. The big players don't care much about cost, and there are large scale firms that compete for the larger EED contracts. But what about the cases that have an EED component without a Microsoft budget?

What if your case involves the cheating spouse? Or the business partner who makes off with the client list on disk? Or the systems administrator caught with tons of child pornography, the help desk administrator who is accessing the boss's confidential files, the parents worried that their daughter or son is in over his or her head

with an online romance? All of these situations come to the general practitioner, the commercial lawyer, the litigator, the family lawyer. In these types of cases, who should you turn to?

The Price of Expertise

A good EED expert will cost between \$150 and \$400 an hour. However, price does not necessarily relate to qualifications or experience. If an expert charges less than \$150, you should wonder how he or she meets overhead expenses and whether the expert will be there to testify for you in two years. If the expert charges \$400 or more an hour, you should be getting top-notch credentials, and it should be a case you think is headed for testimony and trial.

The major factor that should influence your decision as to whether you want a large scale discovery firm or a smaller enterprise is the size of the case and the amount of electronic evidence. Break out the big guns for a case involving millions of e-mails or a large corporate network. For more modest cases involving less discovery, a smaller firm that provides data forensics work will be more than sufficient in addition to being faster and cheaper.

Factors	Big EED Firm	Smaller EED Firm
Large volume of evidence	X	
"Needle-in-haystack" large corporate network	X	
Testimony required	X	X
In a hurry		X

Picking the Wrong Expert

It can be mind boggling to try to figure out what sort of experience and training your EED expert should possess. Many putative experts throw around multiple certifications that have very little to do with EED, and many certifications require little as far as education and experience. Some very able experts possess few certifications and are self-taught while others may appear comparable to Albert Einstein on paper but fall apart on the stand.

Lawyers who do not choose an EED expert wisely can get burned. Having others hold the credentials of your experts up to scrutiny can be embarrassing—and being embarrassed by your expert is the last thing you want, especially in the courtroom. Consider the following example, straight from the record:

Q: *I wish I could say I just had a few questions for you, but, actually, I think I have quite a few. All right. Ms. Expert*, your only formal education is an associate's degree; is that correct?*

A: *I have an associate's degree, yes, I do.*

Q: *And you took no computer courses during the course of obtaining that associate's degree, correct?*

A: *Not obtaining that associates degree, I did not.*

Q: *And you are not a certified forensic examiner, correct?*

A: *You can only be a certified forensics examiner if you are a police officer.*

Q: *But you are not a certified forensic examiner, correct?*

A: *I am not a police officer, nor a certified forensics examiner.*

Q: *And you have no other certifications, correct?*

A: *No, I do not.*

Q: *Okay. And you have only been working in the area of digital forensics [for a year], correct?*

A: *That is correct.*

Q: *Okay. And prior to that, you were a dental assistant—*

A: *Correct.*

Q: *— is that correct? All right. And you*

indicated that your training came from a course by the name of Key Computer?

A: *That's correct.*

Q: *All right. And you have not completed that course, correct?*

A: *No, I have not.*

Q: *And you were last active in that course in May of 2002; is that correct?*

A: *I believe that's correct.*

Q: *And you—you talked a little bit about EnCase?*

A: *Yes.*

Q: *Okay. And you've had no formal training in EnCase, correct?*

A: *That is correct. EnCase will only train police officers.*

Q: *All right. So it's your testimony that EnCase will only train law enforcement?*

A: *As far as I know, that is correct.*

Q: *All right. And you have no formal training on Mackintosh [sic] computers, either, right?*

A: *No, I do not.*

Q: *And you indicated that you testified in—you've testified in court once before?*

A: *Yes, I have.*

Q: *Okay. And was that in April of this year?*

A: *I believe it was in April of this year.¹*

* Name changed here.

How would you like to be the lawyer who employed that expert? Can you imagine the pain of watching as your adversary and your witness destroy whatever credibility you once had?

How to Identify the EED Expert for Your Case

Choosing a smaller, local EED expert can be tricky. If you are not fully versed in the often complicated and more esoteric

issues associated with electronic evidence, its capture, and its analysis, it is a good idea to either hire another attorney to broker the hiring of the right firm or to hire an EED firm that employs an attorney who is experienced in the field. Currently, there are no certifications or associations of lawyers that specialize in EED. Indicators that the lawyer is qualified include his or her experience and training in EED and recommendations from past clientele. The lawyer should be able to tell you the potential strengths and weaknesses of the evi-

dence you seek and give you tips on how you might use it. The lawyer should also be able to provide you with information about the opposing expert and help you to develop questions

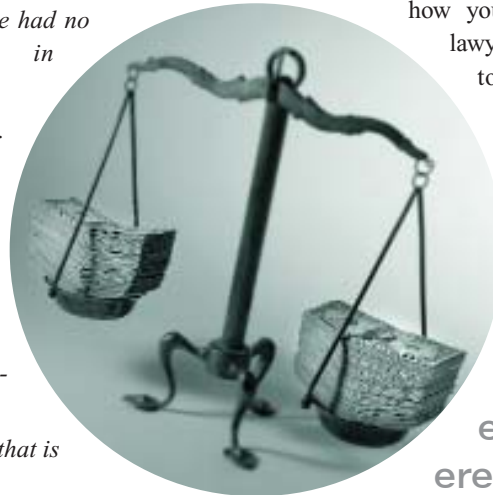
It is prudent to check an expert's references....Some phone calls up front may take a few minutes but they could save thousands later on.

for both the opposing expert and your own.

A lot can ride on the qualifications of your EED firm and the individual expert. If you don't feel comfortable speaking the language, you'd be well advised to employ the assistance of an attorney who does. Many EED experts can explain their work so that the average attorney can understand it and appreciate how to exploit their findings to a client's greatest advantage. Others benefit from having an attorney on staff to serve as a liaison with their attorney clients. EED can involve very thorny legal issues: Not only are these issues best appreciated and explained by a fellow lawyer, but a lawyer experienced in the field is most likely to spot them.

For instance, chain of custody and authentication issues frequently come up in

(Please see next page)



EED cases. When the evidence itself is damning, the best course of action is to try to get it thrown out because it was tampered with or improperly handled. Information technology, as opposed to information security, personnel are notorious for mishandling electronic and digital evidence. Many times they conduct improper, undocumented examinations of evidence or seize evidence without properly documenting their actions to ensure an unbroken chain of custody. Whatever firm you employ should be close enough to the actual seizure of the evidence to be able to ensure an adequate chain of custody record. Some companies and universities have established new operational units with digital forensic capabilities to do this while other companies have firms on retainer should an incident arise.

For that reason, retired and active law enforcement officers who conduct EED examinations are sought after: They are well trained in investigative techniques and appreciate the importance of maintaining a chain of custody and documenting their actions.

EED Challenges for Criminal Defense Lawyers

Criminal defense attorneys should note that it can be very difficult to find experts who possess qualifications comparable to prosecution experts in criminal cases. Codes of ethics for many certifications and membership groups exclude anyone known to associate with hackers or who work on criminal defense cases. Active law enforcement officers may be prohibited by the terms of their employment from working for the defense. Aside from the issue of fairness and availability of assistance in one's defense, these situations put criminal defendants in a position where they must employ experts who come to the case from a completely different perspective. However, this isn't necessarily a bad thing, and there are many well-qualified professionals to conduct examinations of electronic evidence. As all attorneys should, the defense should choose an expert wisely.

In cases where a criminal defendant must find an expert, it is advisable to seek out someone who has experience testify-

ing in similar cases and in EED. In lieu of typical law enforcement certifications, opt for higher academic achievement and publication in scholarly and digital forensic publications. Whenever you stray from reliance on certifications and resumes, extra effort into reviewing any past testimony is essential.

Expect Experience

There is an ongoing debate within the EED community regarding the minimum standard of experience and training required of experts. One argument suggests that the expert should have law enforcement and investigative experience with a minimum amount of EED training. The other key argument propounds that academic credentials in computing are necessary and that appreciation for chain of custody and investigative techniques can either be learned by the examiner or enhanced through the supervision of a qualified attorney. Both sides have merit, and while that may seem to complicate selecting the right expert, the prudent attorney will be able to evaluate credentials so that he or she gets an expert with the right balance of both technical and legal expertise.

There is no substitute for experience. In a constantly evolving field such as EED, there are new "experts" tacking up shingles every day. Ask how many cases the firm has handled, and what type of cases they were. It is prudent to check an expert's references, even if they are provided by the firm. Some phone calls up front may take a few minutes but they could save thousands later on. Ask whether the firm will be conducting the examination itself or if it plans to subcontract out the work. This, of course, can be controlled through a properly drafted agreement, but it's important to know that your firm might farm your case out if you do not prohibit it in writing.

If you can, determine the experience and

training of the examiner who will be analyzing your evidence. As is the case in some forensic labs, the person who will testify is not necessarily the person who actually examined your evidence. If your opponent gets "feisty," probing the chain of custody and the like, it could poke some holes in your expert's credibility. At the very least, in a field in which most are not familiar, any chink in the expert's armor can jeopardize the strength of his or her testimony.

A prospective EED firm should be able to provide you with at least one sample report, which should be comprehensible. If you can't understand the report when *you* read it, how will the expert be able to explain it on the witness stand to jurors or to the judge? Clarity is critical.

Meet the person who might testify. This may sound silly, but there are many experts in the field who you would be reluctant to put on the stand. Imagine employing an EED examiner who seems highly qualified over the phone. The credentials look great. The picture on his Web site looks respectable, even scholarly. When he shows up to testify, his clothes are disheveled, he has shifty eyes, and he



If you can, determine the experience and training of the examiner who will be analyzing your evidence. As is the case in some forensic labs, the person who will testify is not necessarily the person who actually examined your evidence.

(Please see page 33)

Common EED Certifications and What They Mean

EnCase Certified Examiner (EnCE): EnCase is a software program owned by Guidance Software. EnCE is a designation bestowed on private practitioners and public sector examiners who successfully complete a combination of training and experience as well as an examination. The benefit of EnCE is that it demonstrates that the person is proficient in using EnCase software. Although the software can be expensive, the certification candidate need not purchase it to achieve the EnCE seal of approval. All of the EnCase trainers are former law enforcement personnel who have conducted forensic examinations for their former agencies.²

Certified Information Systems Security Professional (CISSP): The CISSP is issued by the International Information Systems Security Certification Consortium, Inc. (ISC2). Candidates must have three or more years of work experience in information systems security and pass a test that measures their knowledge in ten areas of information systems and security. CISSPs are required to complete a minimum number of continuing education credits during each certification period.³

Certified Computer Forensic Examiner (CFCE): This certification is only available to police officers and some law enforcement personnel and is issued by the International Association of Computer Investigative Specialists (IACIS). There are no prerequisites for IACIS training, as the association claims to provide most of what the student needs to learn. After two weeks of training, candidates work on nine forensic problems to complete the training.⁴

Certified Computer Crime Investigator (basic) (CCCI [basic]): Offered by the High Technology Crime Network, this certification is open to those involved in law enforcement and to the private sector. It requires two years' investigative experience or a college degree and one year of experience. Eighteen months' experience must be directly related to technical incidents or crimes. The candidate must have attended at least forty hours of computer crimes training. Applicants must document at least ten cases they have been involved with. Note that there is no testing. Applicants need only assert that they have the requisite experience and training for the certification and pay the fee.

Certified Computer Crime Investigator (advanced) (CCCI [advanced]): Offered by

the High Technology Crime Network, this certification is open to those involved in law enforcement and to the private sector. It requires three years' investigative experience or a college degree and two years' experience. Four years' experience must be directly related to technical incidents or crimes. Candidates must have attended at least eighty hours of computer crimes training and document at least sixty total cases they have been involved with as an investigator. Applicants need only assert that they have the requisite experience and training for the certification and pay the fee.

Certified Computer Forensic Technician (basic) (CCFT [basic]): Offered by the High Technology Crime Network, this certification is open to those involved in law enforcement and to the private sector. It requires eighteen months' experience directly related to computer forensics. Candidates must have attended at least forty hours of computer forensics training and successfully complete a written exam. Applicants must also document at least ten computer forensic cases in which they have been involved. In addition to the exam, applicants need only assert that they have the requisite experience and training for the certification and pay the fee.

Certified Computer Forensic Technician (advanced) (CCFT [advanced]): Offered by the High Technology Crime Network, this certification is open to law enforcement and the private sector. Four years' experience must be directly related to computer forensics. Candidates must have attended at least eighty hours of computer forensics training and successfully complete a written exam. Applicants must also document at least sixty computer forensic cases in which they have been involved.⁵ In addition to the exam, applicants need only assert that they have the requisite experience and training for the certification and pay the fee.

Certified Computer Examiner (CCE): The CCE is offered in association with the International Society of Forensic Computer Examiners, and there are several levels of



Opt for experience testifying. If you can't find a good former law enforcement expert with a proven record of testimony in reported cases, which would be unusual, opt for presence, charm, academic credentials, and publications in the field.

certification. Baseline standards include that candidates have no criminal record, meet minimum experience and training requirements, abide by the association's code of ethics, pass an online examination, and successfully examine three test cases. Certified individuals are required to pass proficiency tests every two years.⁶

Seized Computer Evidence Recovery Specialist (SCERS): SCERS training is reserved for law enforcement personnel only, that is, active police officers and examiners working for a law enforcement agency, and is offered through the Federal Law Enforcement Training Center. Originally developed for Internal Revenue Service agents, SCERS training became a model for all federal law enforcement EED personnel and was eventually opened to some state and local police. It involves two weeks of intensive training in seizing and searching electronic evidence. SCERS candidates must successfully pass a graded test to graduate.⁷

Certified Forensic Computer Examiner (CFCE): The CFCE certification is offered by the International Association of Computer Investigative Specialists.⁸ The certification is only open to law enforcement personnel, that is, active police officers and examiners working for a law enforcement agency. IACIS offers two weeks of training and requires successful completion of a sample examination, which candidates do on their own once they return from the training.

WHAT TO LOOK FOR IN AN ELECTRONIC EVIDENCE DISCOVERY FIRM

(CONTINUED FROM PAGE 24)

looks at his feet when he talks. Your heart sinks as you watch the reaction of the jurors: They are distracted by his looks and mannerisms and aren't hearing his testimony.

Finally, ask the firm about price. Do they charge a retainer, and, if so, will it be likely to cover the exam or is it just a down payment? What have they charged in similar cases? Ask if they will charge you for their time alone or for their time plus machine time. Machine time is the time spent while the examiners are eating dinner with their families or fast asleep in their beds while their computers create duplicates of original evidence or search for evidence.

Summary

- Consult another lawyer who is experienced in EED to recommend a firm for the job and to consult on evidence issues—even if you are technically savvy.
- Review the experience and training of anyone who will be analyzing your evidence.
- Opt for experience testifying. If you can't find a good former law enforcement expert with a proven record of testimony in reported cases, which would be unusual, opt for presence,

charm, academic credentials, and publications in the field.

- Get a sample report (very important).
- Meet the person who will testify before you engage his or her services.
- Request detailed pricing information. **CL**

Monique Mattei Ferraro is an attorney with the State of Connecticut Department of Public Safety Computer Crimes and Electronic Evidence Unit. She is also in private practice and can be contacted at monique-ferraro@optonline.net. She teaches Criminal Justice at Post University, Kaplan University, American InterContinental University, and Corinthian College. The opinions expressed in this article are solely those of the author.

Notes

1. From *State of Washington v. DeGross*, Super. Court No. 02-1-960-7 (May 29, 2003).
2. More information is available online at www.guidancesoftware.com.
3. More information is available online at www.isc2.org.
4. More information is available online at www.cops.org.
5. More information on certifications is available through the High Technology Crime Network and online at www.htcn.org.
6. More information is available online at www.certified-computer-examiner.com.
7. More information is available online at www.fletc.gov.
8. More information is available at www.cops.org.

Insuring Attorneys for Over 20 Years.

- ◆ MLM has been a provider of legal malpractice insurance since 1982.
- ◆ "A" (excellent) rated by A. M. Best since 1992.
- ◆ Since 1988 MLM policyholders have received over \$23 million in dividend payments.
- ◆ MLM is a direct writer; you work directly with a company representative.
- ◆ Outstanding customer service which is reflected in a renewal rate greater than 95%.
- ◆ Free legal technology advice and practice management consultation.

Save 10% by applying online at www.mlmins.com.



MINNESOTA LAWYERS MUTUAL
INSURANCE COMPANY

800.422.1370

www.mlmins.com