# Finding Wyatt Earp:
# Your Digital Forensics Expert

By Sharon D. Nelson, Esq. and John W. Simek


Wyatt Earp, c. 1886

You are about to enter the OK Corral of litigation. The stakes may not be life and death, but they're high. You have a litigation team – your own version of Doc Holliday, Virgil Earp and Morgan Earp. The other side is also formidable, the modern day equivalent of the Clantons and the McLaurys. Both sides are well armed and ready for bloodshed.

In the ensuing battle, more often than you might imagine, the winning difference in cases involving electronic evidence is the skill level of the digital forensic expert. Whose expert will the jury or judge find more credible?

It is at this juncture that you hope fervently that you haven't bet your client's monies and case on Ike Clanton. You hope your guy is Wyatt Earp himself, imperturbable, flinty-eyed, and deadly accurate. But where oh where do you find the Wyatt Earps of digital forensics?

Scarcer than rubies are talented digital forensics experts who are also skilled at writing expert reports and giving court testimony. So how do you find a good expert when you have electronic evidence in issue? This can be a daunting task and the right selection may depend upon a number of factors including what's at issue in the case, the budget, the geographic location of the expert, and balancing the relative credentials of the experts under consideration. In short, reach for your bottle of Advil. Mistakes are frequent.

Here are the extremes. At one end, you have the major players – with big price tags and a horrendous disparity of quality between their employees. At the other end, you have Joe, formerly a plumber, who fiddles with computers at night and thinks that digital forensics is cool. He takes a course in it, perhaps even gets a meaningless certification from the vendor, and then promptly hangs out his shingle, advertising his service at "blue light special" rates.

Do you pay a fortune for the big name players? Do you take a chance on Joe and his brethren?

Regardless of the size of the firm you choose, here are some of the factors you should consider in selecting the specific forensic technologist expert for your case:

1. **Forensics certifications**. Currently, there are several digital forensic certification available to private firms. One is the EnCE (EnCase Certified Examiner) issued by Guidance Software. Another respected certification is the Certified Information Forensics Investigator (CIFI) issued by the International Information Systems Forensics Association (IISFA), a non-profit organization. Another vendor neutral certification is the Certified Computer Examiner (CCE) issued by the International Society of Forensic Computer Examiners (ISFCE). Another noted certification is the GIAC Certified Forensic Examiner (GCFE). More certifications are emerging and will gain credibility over time, but in the private sector, the four mentioned certifications are the ones to look for. A caveat: many less than honest folks will claim certifications on their CV when the truth is that they took classes or had training courses – no real meaningful certification was granted, just a "certification of attendance." If you see a certification you don't recognize, find out whether a written exam was required. Did the applicant have to prove some minimum time that he/she had been involved in digital forensics? Was the expert certified in digital forensics or merely in the use of a particular forensics tool? What organization issued the certification? Who was on the faculty? Was a practical hands-on component part of the testing? Is there a recertification component?

2. **Technical certifications**. A good forensic technologist will have a lot of letters after his/her name, indicating a broad range of certifications with a number of different technologies. If you see no certifications, or a "base-level" certification (such as A+), you do not have an individual with a wealth of experience. If the expert is (just by way of example – there are many, many valuable certifications) a Certified Novell Engineer, Certified Cisco Network Administrator, Microsoft Certified Solutions Associate, Microsoft Certified Systems Engineer, Microsoft Certified Solutions Expert, Certified Information Systems Security Professional, NT Certified Independent Professional, Certified Handheld Examiner and a Certified Internetwork Professional, you've got someone with an expansive technical background.

3. **The CV.** Get the expert's CV early on and study it. Don't be afraid to ask questions. Does it show that the expert has spoken at a lot of seminars and/or written a lot of articles? Those who present or teach frequently and have to answer questions on the fly tend to be excellent testifying experts. Also, teaching and authorship frequently add credibility with a judge or jury. What is the expert's educational and professional background? Is this a broad-based technologist or someone who is a new college grad and wet behind the ears or with only a narrow sliver of technical knowledge?

4. **The Jack of All Trades.** Beware the individual who claims multiple disciplines. Whether a private detective, computer repairman, or software engineer, or some

combination of many things, a forensic technologist worth having is generally billed as a forensic technologist and does not offer a Chinese buffet of services.

5. **Point-and-Click.** Beware of point-and-click experts. Some experts merely know how to "drive" the various forensic software tools by clicking a mouse on menu items. The software then spits out a report or analysis. This can be a dangerous situation because the expert presents the various reports without a clear understanding of the underlying data. A true expert will understand the electronic evidence that feeds the analysis and will correctly interpret the results. All too often the point-and-click expert can't explain the significance of certain elements or puts too much weight in meaningless information.

6. **Court Qualifications**. The last thing you need as an attorney is an expert who hasn't qualified as an expert. Good experts have qualified in multiple courts and they are all listed on the CV. Mind you, most cases of any kind tend to settle, so even the best of experts may only appear in court several times a year. However, it is wise to be wary of someone who has only qualified in one court – or none at all. You don't need a greenhorn cutting his/her teeth on your case.

7. **Confidentiality**. Remember the line from the gossip columnist in the movie *L.A. Confidential*? "Off the record, on the QT, and very hush-hush." Not all cases are shrouded in secrecy, but a fair proportion of them are. There are well known figures getting divorced, major companies with proprietary information at issue, public figures in the headlines and people charged with felonies. Make sure the expert you pick has a confidentiality clause in the retainer agreement and don't hesitate to ask the expert to sign your own confidentiality agreement. Remember as well that the expert may be working your case with others and that the entire firm should have an impeccable reputation for keeping client secrets. During the course of a major case where the expert has been identified, the press will undoubtedly come sniffing around the expert probing for information. A good expert knows the standard answer, "I'm sorry, I have no comment" and is as immoveable as the Great Wall of China.

8. **Geography may not matter**. How often attorneys forget that this is the electronic era! You can maintain chain of custody perfectly well by shipping a computer from California to New York if that's where the best expert is located. While it is true enough that local experts are often preferred where monies are tight and travel expenses may be in issue, many lawyers lose sight of the value of having the best possible expert, irrespective of location. If the case has a significant amount at state and/or may well end up in trial, it is a disservice to clients to restrict them to local experts. Those experts who are well known in the field have clients across the nation and beyond because their expertise is so often sought.

9. **English 101 and 201**. An expert MUST speak the English language. We have many wonderful friends who are of foreign descent and brilliant, but their English will not pass muster with a mixed ethnicity jury. Their accent is just too

pronounced for many folks to comprehend, especially for those who may have learned English as second language. That's English 101, being able to speak the language clearly. English 201 is being able to speak about highly technical matters in lay terms, with analogies that a judge or jury can understand. Geek-speak is worse than useless in a courtroom situation. You will come to revere an expert who easily makes analogies in terms of TV, cars, sports and other things that represent part of Joe Q. Public's everyday life.

10. **The price tag**. Digital forensics is not cheap. Small cases may run in the $5,000-$10,000 range, but larger cases can hit six figures with astonishing rapidity. It is almost never possible to quote a probable final figure, because the technologist has not yet seen the "size of the elephant." It will generally require some time into the case before it is possible to let a client know how much work will ultimately be involved. It is, as we all know, often the same predicament lawyers face when trying to give clients a rational estimate. As a general rule, the larger the forensics firm, the larger the bill. It is not uncommon to pay as much as $500/hour in the largest firms. In high quality but smaller firms $300-$400/hour may be a more common charge. If the firm you're looking at charges less than $200/hour, you probably want to raise your eyebrows and seriously investigate the firm credentials, references, number of courts qualified in, standing in the industry, etc. Heed this advice well: some technologists bill fairly. They turn their clocks off while a process is running and go work on someone else's case. They account for their time accurately and precisely. On the other hand, there are those (often with lower rates), who charge you for every moment they are at work – and sometimes beyond. We have seen countless invoices for 9-10 hours a day at work, with no time removed for going to lunch, bathroom breaks, chatting with colleagues, meetings, etc. Frequently, we have found that those with lower rates compensate by billing for more hours. A conundrum for a client. Is the lower rate really going to mean a lower bill? Or will the higher rate, accurately applied, result in a smaller total? In the end, getting references is your best bet here. C*aveat emptor*!

11. **References, references, references**. There is no better way to secure a good expert. Ask your potential expert for references and then make sure you follow up with those references. Did the expert do a thorough, professional job? Was the expert responsive when contacted? Was the work completed on time? What was the quality of the expert's report? Did the expert make a credible witness? Was this an expert amenable to being "spun?" Experts who are "experts for hire" are a nightmare in court. If your candidate has the attitude that "the truth is the truth," you may not want that truth in court, but at least you will know the realities of your case, its strengths and weaknesses. Did the expert stay within budget (not always possible) or at least alert the client of additional costs before incurring them? Perhaps the number one complaint heard about experts involved in electronic evidence is that costs spiraled out of control without notification to the law firm, resulting in a client highly perturbed with its bill --- and its law firm.

At the end of the day, you want a good result at a fair price. Don't be penny wise and pound foolish. Pay good people good monies and you'll have a credible result – you may not get the answers you want, but what you get will hold up in court. Make no mistake about it – in e-evidence cases, it frequently comes down to a duel between the experts. Your guy gets blown away or their guy gets blown away. What you want is for your guy to be Wyatt Earp and the other side's guy to feel like one of the Clancy brothers staring down the barrel of Earp's "Peacemaker." You will be a lot happier in the courtroom's O.K. Corral if you have the biggest gun!

*The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com*