

Finding and Selecting A Computer Forensic Expert

by

Gregory L Fordham
CPA, CIA, CCE, Sec+, MCP, Live, Stego



WWW.KNFCON.COM

2550 Northwinds Pkwy, Suite 275
Alpharetta, GA 30004
770-642-0311

TABLE OF CONTENTS

Introduction.....	1
Finding a Computer Forensic Expert.....	2
Selecting a Computer Forensic Expert	3
Criminal versus Civil	3
Presentation Skills.....	3
Forensic Tools.....	4
Case Specifics	5
Industry Specifics.....	5
Relevant Experience	5
Training.....	6
Educational Background.....	6
Certifications.....	7
Conclusion	8

FINDING AND SELECTING A COMPUTER FORENSIC EXPERT

Gregory L Fordham
CPA, CIA, CCE, Sec+, MCP, Live, Stego

Introduction

As digital evidence continues to become more common in litigation, so has the need for computer forensic experts.

Computer forensics is often defined as the application of numerous science and engineering disciplines to the legal problem of digital evidence. Said another way, it is the application of computer skills and knowledge in a litigation environment to examine, analyze and interpret computer related evidence.

Although most people consider computer forensics to equal imaging and analyzing computer hard drives, this is actually only a portion of computer forensics based on the above definition. Under the above definition virtually anything digitally or computer related could be computer forensics once the problem is placed in a litigation context.

Computer forensics can be distinguished from another discipline used by lawyers known as electronic discovery. Electronic discovery is the collection and production of digital evidence in a litigation environment. It can be distinguished from computer forensics in that it lacks the examination, analysis and interpretation of the data. Rather, e-discovery considers only the relevancy of the data to the legal matter as well as its compliance with various legal criteria such as “attorney client privilege” and “attorney work product”. When viewed on a time line, electronic discovery can be the precursor to computer forensics, since it can provide the data that the computer forensic expert will examine.

Another term worthy of consideration is data recovery. While computer forensic experts may utilize data recovery, data recovery is not computer forensics. Computer forensics is practiced in a manner that preserves potentially relevant evidence. Data recovery by itself does not claim to provide this safeguard. For example, both the data recovery expert and the computer forensic expert can use the same tools and skills for recovering deleted data. The computer forensic expert would employ practices that prevent the recovery of deleted data from damaging or

destroying other potentially relevant evidence. The data recovery expert would not necessarily take such precautions. Rather, the data recovery expert may just recover the data to any available free space on a medium.

In some areas of modern litigation, the entire case is driven by the findings of computer forensic experts. Even in garden variety e-discovery cases, where one would think that the challenges are simply the efficient and timely exchange of documents, the aid of a computer forensic expert can be essential to assess document authenticity, production compliance and the existence of spoliation.

Once the need for a computer forensic expert is recognized, the next likely hurdle will be how to find and select one. To the uninitiated, this may seem no more complicated than an inquiry with a colleague. However, there are more things to consider, particularly now as the number of those claiming to have this expertise grows to meet demand. The following sections provide guidance to the litigator on finding and selecting a computer forensic expert.

Finding a Computer Forensic Expert

Once the lawyer has determined to use a computer forensic expert the next likely hurdle will be how to find one. Of course, there is always the old fashion way that is probably used most by lawyers. That is asking around with other firm members and colleagues about experts that they may have used and would recommend.

Performing searches on the internet is another common method of finding experts. If their websites exist then evaluating the content of those sites can help identify candidates.

Besides searches of the internet, those with access to case decisions can also search those for instances where experts are identified.

Of course beyond that are the usual directories. Some of the better known are Martindale Hubbell, AMExperts and then various industry or geographically specific directories such as construction industry directories or local bar association directories.

As computer forensics has become more common, there are also professional associations that can provide member lists. For example, the International Society of Forensic Computer Examiners is one professional association where individuals can be found. In addition there are also tool specific certifications like guidance Software's EnCE [Encase Certified Examiner] and Access Data's ACE [AccessData Certified Examiner].

Selecting a Computer Forensic Expert

Once you have located potential candidates, or at least sources for potential candidates, the next step will be selecting a computer forensic expert. There are a number of features that can influence a selection decision. Some of those criteria are litigation background such as criminal or civil; the education background, training, tools, nature of the case and industry specifics.

Criminal versus Civil

One might consider using an expert with a law enforcement background. These individuals tend to make great witnesses for juries because of their instant credibility.

If the case is a civil matter, however, there are other things to consider. After all, the differences between criminal and civil cases are more than the law. Indeed, the capabilities of the experts are shaped by the procedural differences as well as the cultures spawned by those procedures.

In criminal cases the bar is higher than in a civil matter. In addition, prosecutors can have larger case loads than their civilian counterparts. Both of these factors can pressure them and their experts to focus on the low hanging fruit.

The net result is that an expert grounded in criminal cases involving child pornography may be more accustomed to finding the sure thing than going the extra mile to pursue issues that require research, testing, extensive analysis or marshalling complicated fact patterns.

Another difference is that in a civil case the opposing side often has considerably more notice of the impending production than a criminal defendant served with a search warrant. As such, in a civil matter it can be more important for the computer forensic expert to know how to find traces of what had been on the computer than finding the files themselves.

Also, criminal experts may not be accustomed to the discovery that occurs in civil proceedings. Thus, they may not be used to report writing, giving depositions and revealing and supporting their evidence and opinions prior to testifying at trial.

Presentation Skills

Another factor to consider is presentation skills. An expert's presentation skills are not just important while testifying at trial. Indeed, they are important throughout the entire litigation lifecycle that can include briefings with the legal team and the client as well as formulation of tests and procedures for advancing the case.

Interestingly, advancing the case is not just about sifting and interpreting evidence. It can include using his expertise to counter the obstacles devised by opposing counsel to stifle discovery

So, the expert must fill many roles. He must be a teacher and a strategist. It is not enough to find interesting artifacts. The expert must be able to educate the lawyer about differing ways to obtain relevant evidence that is important to the case as well as the significance of his findings.

Delivery of the expert's findings is also an important part of his presentation skills. Many of the forensic tools used by experts possess report writing tools. While these tools are good for experts, who already understand all of the attributes they contain, they are not typically good for lawyers. Often they are no more than raw data dumps. Unless the lawyer is familiar with these reports or even the data that they contain they will likely be useless to the lawyer.

In terms of strategy, there are two ways that the expert can help. The first is uncovering the flaws in the opposing side's claims that requests are overly burdensome. The second is devising techniques for sifting data efficiently when opposing counsel has delivered "quicksand".

Forensic Tools

Understanding the tools used by the expert can also be important. This facet can involve issues related to the kinds of tools, the variety of tools and the number of tools.

With respect to the kinds of tools, the litigator may want to determine whether the expert has invested in mainstream forensic tools or are they getting by with freeware and other low priced alternatives. While it is nice to avoid needless markups, the lower priced tools are also commonly less feature rich and will require more labor hours to obtain the same results that might be automated in the higher priced tools.

Again understanding the specific tools owned and used by the examiner can be useful. Some tools are stronger in certain functions than others. So, again, it becomes important for the forensic expert to have diverse resources from which he can draw depending on the requirements of the case.

Forensic analysis tools are not the only kind of tool in the expert's arsenal. In large complex cases it is also the ability to manage the data and marshal the facts. While spreadsheets, as an example, provide robust analysis capability they are size constrained. So, in large cases spreadsheets lack adequate horsepower. In large cases, database applications can become much more essential.

So, in large case the litigator may want to assess how well equipped is the expert to manage large volumes of data and analyze them. Even the forensic tools can have practical size limits such that the data must be piecemealed from those applications and placed in other, more capable data management systems.

Another issue could be the number of licenses of its tools a forensic examiner owns. In large cases, throughput can be essential and multiple licenses a must.

Another category of tools are those that the litigator can use to provide data to the litigator. If the data are comprised of lists then spreadsheets are litigator friendly. But what happens when the lists exceed the capacity of the litigator's spreadsheets. How about different data types such as e-mails. Should those be provided as PSTs, HTML, or MSG type documents? Indeed there are many questions about how the expert can support the litigator's needs in the kinds of tools that the litigator is capable.

Case Specifics

Case specifics also provide a distinguishing attribute for the expert. After all, just like litigators can acquire specialties so can computer forensic experts. For example, the ideal expert for a computer security and network intrusion case may not be the ideal expert for a trade secrets, bankruptcy or family law matter.

The complexity of the case can also affect the skills of an expert. Perhaps the issues are rather simple or one dimensional. For example, maybe all that is needed is someone to determine when the computer was last started or whether a particular file exists on the media. These kinds of issues could be satisfied with a much broader range of experts and with less sophisticated skillsets.

So, case specifics can dramatically affect the selection process. What will be challenging for litigators is identifying and understanding how those case differences will manifest themselves in the skillsets of a forensic computer expert.

Industry Specifics

Industry specific background can also be helpful for the computer forensic expert. Activities, systems or artifacts that might otherwise go unnoticed could be recognized by the expert familiar with that industry. Also, experts familiar with an industry may be able to recognize omissions in preservation or production as a result of their knowledge.

Relevant Experience

The analysis of the expert's relevant experience can be another important discriminating factor. He could have both or either related work experience but how do either of these fit into a

litigation environment. For example, even if the expert has worked in other litigation cases, what does he do to validate a production. Does he take steps to identify omissions and/or manipulations or does he simply proceed with what has been given.

Can he work with imperfect information? Is he able to reverse engineer the work of opposing parties without documentation or other information gaps?

Training

Training is another area that the litigator can use to distinguish computer forensic candidates. In this regard there are a number of training directions that the litigator may find of interest. Essentially there are the general training classes and there are the tool specific training classes.

The general training classes can involve fundamental issues such as file systems, operating systems, and software applications such as e-mail, application databases, and software applications in general. Such classes would reveal how these subjects work, how to interpret their metadata and how to extract and handle their artifacts.

As an example, consider the situation where the computers to be examined are Microsoft Windows based machines versus Apple Mac machines. The file systems that accompany these two different devices behave differently and leave different kinds of artifacts. Knowing about these artifacts, where they reside and how to interpret them can not only affect the expert's opinion but influence the budget required to interpret them.

The other area where training can be influential is on the tools used by the expert to develop his own opinions as well as refute those of the opposing side. These days there are a number of forensic tools and no single tool will perform all evaluations. So, in order to perform a comprehensive examination the expert will likely need to have several tools in his toolbox and needs to be familiar with them whether through self training and seasoned use or formal training.

The need for tool familiarity is not limited to the performance of the expert's own work. Rather, he will also likely need this familiarity to understand and evaluate the work of the opposing expert.

Educational Background

Evaluating a computer forensic expert's educational background is not like evaluating those of a licensed engineer, medical doctor or accountant. By comparison to these other professions, the entire computer industry is relatively new. Someone with twenty years experience dates to a time when there was not even an abundance of degreed offerings, if any.

While there are more generalist degree programs today such as computer science, information systems, software engineering and the like, even they are not designed with the skills that

computer forensic experts are likely to use. So, there may be no real advantage to experts having such credentials. Furthermore, educational degrees are not even required in order to qualify as an expert, although the litigator may want to use such credentials as a means to separate candidates.

In more recent times, there are degree programs in computer forensics that are starting to appear in college curriculum. While these are likely to provide a good foundation to those having them, again they are only a foundation. If anything, their usefulness may signal the seriousness at which the holder, pursues his career. On the other hand, in some esoteric areas it is unlikely that a worthy expert would have need of such designations.

Certifications

Like educational degrees, professional certifications in computer forensics are rather a recent commodity. So, it could be likely that computer forensic experts will not have forensic certifications. Of course depending on the nature of the case a forensic certification may not be necessary.

Computer forensic certifications generally deal with media files systems, operating systems, and interpretation of their artifacts. In some scenarios such as network or software functionality the classic computer forensic skillset may not be needed. Rather, more traditional computer system operation is all that is necessary.

So, litigators should realize that with respect to computer forensic certification there are relatively few and most of those are tools specific. Examples of tools specific certifications are the Guidance Software, the makers of EnCase, EnCE [EnCase Certified Examiner] and Access Data's, the makers of the Forensic Toolkit, ACE [AccessData Certified Examiner]. Of course there are still others but these two examples are probably the best known.

Examples of the non-tool specific certifications are the Certified Forensic Computer Examiner (CFCE) that is offered to law enforcement personnel only by IACIS. Another generalist certification is the Certified Computer Examiner (CCE) offered to anyone by the International Society of Forensic Computer Examiners (ISFCE).

Beyond these classical forensic certifications are numerous operational certifications. Some of these include those offered by vendors like Microsoft such as the Microsoft Certified System Engineer (MCSE) and Microsoft Certified Professional (MCP) to name a few of the Microsoft certifications. Many other vendors offer their own certifications as well such as Cisco Systems with their Cisco Certified Network Administrator (CCNA).

There are also generic certifications offered by industry associations such as the Computer Technology Industry Association (CompTIA).

Conclusion

Despite the increasing availability of computer forensic experts, selecting them is becoming more difficult. It is not that there are fewer of them. Quite the opposite is true. There is much more to choose from and as such the search can be more complicated and time consuming.

Furthermore, computer forensics is not some kind of single subject discipline. While most people may think of them as hard drive examiners, the field is much more diverse than that. Also, as computers continue to permeate more and more of our society and legal system, the number of specialties and nuances increase accordingly.

So there is much to consider when selecting the right computer forensic expert. One size does not fit all. Making the correct choice can involve a multitude of considerations.

In the end, however, the right choice for any litigator just depends. But would you expect anything less?