Chapter VII

Preparing the Forensic Examiner for Examination

by Susan S. Kreston

I. "Computer Forensics" Defined

Computer forensics can be defined as having three components. First, it is the extraction of computer evidence without alteration to the original material. Second, it is the impartial examination and analysis of that evidence. Finally, it is the ability to present these findings effectively in a court of law. When deciding on trial tactics and strategy in a case involving computer/digital evidence, one of the areas prosecutors need to address is how to present the forensic evidence to the trier of fact. Within the subject matter of forensic evidence, one of the major questions is will the prosecutor present the examiner as a lay witness, or qualify the examiner as an expert, and if as an examiner, in exactly what field. This chapter addresses the areas of concern when forensic examiners testify, present the pros and cons of expert qualification, and conclude with a list of questions that may assist prosecutors in qualifying a witness.

II. Qualifications of a Forensic Examiner

The qualifications of the forensic examiner should be discussed with the prosecutor well in advance of trial. The concept behind the multidisciplinary approach to investigation and prosecution dictates that the witness and prosecutor are both prepared for the examiner's testimony. As there will be very few examiners who have a degree in computer forensics, or even in computer science, the real-world qualifications that the examiner brings to the investigation should be stressed. Experience and knowledge will usually impress a jury far more than academic titles not accompanied by hands-on practice. By establishing the examiner's title, current assignment, and history in law enforcement, the jury will become familiar with the witness's general qualifications. Pursuing the educational training and background, including any relevant courses and certification the witness has received, any training that the witness provides to others in the forensic community, and any professional organizations, publications, or awards the witness may have will further establish this individual as more than competent to testify. The number of examinations that the witness has performed and whether they have ever testified before, either as a fact witness or as an expert, should complete the foundation.

When deciding whether to qualify the examiner as an expert, certain issues should be weighed and anticipated. First, is there a need to qualify this witness as an expert, or is this really a fact witness? If the witness is simply testifying to what was done in the course of the investigation (e.g. "I found these files here" or "I did not find any files at all"), then there may be no need for expert qualification. An adequately trained examiner utilizing reliable software should be allowed to testify simply as to what was found during the forensic examination without the examiner first being qualified as an expert witness.

Regardless of whether the examiner is qualified as an expert witness, it must be demonstrated that the data or digital evidence was unaltered between the time of its seizure by law enforcement and its examination, as well as throughout the entire examination process. But if for some reason the data has been altered, the examiner will need to explain exactly how and why.

If there is an opinion being offered (e.g., naming of folders and files, or paths through which data is saved showing intent or knowledge, lack of mistake, or impossibility of inadvertent downloading), then the witness must be qualified before rendering that opinion. The benefits of having a qualified expert are that they may render an opinion and may be perceived by the trier of fact as having more credibility. One potential area of difficulty, however, is that at this time there is no single certification or regulatory authority that covers this area. Training and certification may be obtained from any number of reputable organizations (HTCIA, IACIS, SEARCH, FBI CART, RCFLs, NW3C, California Department of Justice, military training), but currently there is no one national standard or accreditation. Attendant to this is the fact that there is no universally accepted "best practice" or "model protocol" in this field. That is not to say that there are no "best practices" publications, one of the best known being that of the Secret Service dealing with seizing electronic evidence.[1] The limited availability of independent software or methodology testing and validation should also be assessed for potential pitfalls. If the witness is not only the forensic examiner but also the investigating officer, the appearance of bias may be present.

These issues may be dealt with by first stressing the certification(s) that the witness does have and that they are the standards within the community. Second, if using software that has been validated in court under *Kelly/Frye* standards,[2] this fact should be stressed. With respect to cross-examination on the question of bias, it may need to be acknowledged that trained forensic examiners are in short supply. Therefore, an investigator may also need to serve as the forensic examiner. In such cases, the use of peer review or meaningful supervisory oversight can assist in verifying examination results.

Finally, being an expert in computer forensics is not the same as being a computer expert. If a witness needs to be qualified, it may be advisable to qualify a forensic examiner at the lowest level of expertise of the particular witness. Forensic examiners are not necessarily and do not have to be experts in "computers." Indeed, it is doubtful that any one person is capable of being a true expert in all facets of computers. A forensic examiner is like many people who work with technology: they have training and experience in a specialized field or area that is part of a bigger picture. If qualified as an expert in the narrow field of computer forensics, the range of questioning to which the witness can be properly subjected is likewise narrowed. Awareness on the part of the forensic examiner and the prosecutor of the exact contours of the examiner's area of expertise may meaningfully assist in the effective presentation of testimony. By not venturing into areas that are outside the witness's true area of proficiency, the potential harm that may be done on cross-examination is minimized.

III. Preparing the Examiner for Trial

The witness should be prepared to discuss the type(s) of evidence examined, how it was analyzed, and the results. Jurors may not be familiar with all the types of evidence present in a given case (e.g., smart cards, thumb drives, thumb nails), so the examiner should explain what these are. The analysis process should be discussed in accurate but broad terms. The jury should get a general picture of the process on direct, but not necessarily an excruciatingly detailed one. If the defense wishes to get into the details of the examination, let them do so during cross-examination. The results of the

examination should be conveyed to the jury in lay-accessible language. Discussing the results of the exam in a juror-friendly manner is crucial. Use of such devices as analogies may assist the trier of fact in understanding important concepts and applying them to the facts of the case at hand. Style and substance are also necessary for effective communication. The witness needs to convey this technical information to a non-technical trier of fact in the way that best facilitates understanding. By discussing the results of the exam in a knowledgeable, objective, conversational, narrative style, the witness increases the likelihood that the jury will be receptive to the witness's testimony.

IV. How to Proffer an Expert

This final section offers a way to proffer an expert and some sample questions that may be used in qualifying the examiner or simply laying the foundation for testimony as a fact witness. Whether or not the witness will be testifying as an expert, these questions may assist in enhancing the witness's credibility, thereby increasing the jury's acceptance of their testimony.

A. Suggested Wording for Proffer

Your Honor, at this time, I would like to tender Investigator "Andrews" as an expert in computer forensics and the examination and analysis of computer evidence.

B. Predicate Questions for a Forensic Examiner

- Please state your name and business address.
- By whom are you employed?
- What is your current rank?
- How long have you worked in law enforcement?
- What assignments have you had in law enforcement?
- What is your current assignment?
- How long have you been assigned to that unit?
- What is your current title?
- What are your specific duties?
- What is "computer forensics?"
- What is a forensic examination as it relates to computer evidence?
- Is there a standard procedure that you follow in performing computer forensic exams?
- Briefly, describe the steps in an examination *(e.g., identification, preservation, acquisition, recovery, reporting).*
- How many examinations have you done to date? *(Keep in mind that one case may have multiple pieces of evidence and each piece of evidence counts as a separate examination.)*
- Do you ever assist other law enforcement agencies in doing forensic examinations?
- What is your educational background? *(If relevant.*)
- Do you belong to any professional organizations? *(Discuss the organization, its membership, and its purpose.)*
- What are your activities within each organization?
- Have you received any training specifically related to computer forensics?
- By whom? *(IACIS, HTCIA, BDRA, ADRA, SEARCH, FBI CART, RCFL, AccessData, Guidance, New Technologies, California Department of Justice, etc.…)*
- Have you received any type of certification by any of those organizations?

- Do you have any other specialized training in the use, operation, and functioning of computers or software? Have you received any additional certification based on that training? *(A+ Net+, etc.…)*
- Have you ever provided training to others on computer forensics? For whom, when, and where?
- In addition to receiving ongoing training, what else do you do to stay current with developments in computer forensics? Listserves? Seminars? Periodicals?
- What is a Listserve and how does it help you stay current?
- Have you ever participated in the execution of a search warrant in the field?
- Have you ever conducted an exam outside the lab setting?
- Have you ever testified before? If so, how often and in what field(s)?
- Have you ever been qualified as an expert witness before? If so, how often and in what field(s)?

ENDNOTES

1. *http://www.secretservice.gov/electronic_evidence.shtml.*
2. *Frye v. United States* (1928) 293 F. 1013; *People v. Kelly* (1976) 17 Cal.3d 24.

Susan Kreston is a consultant for federal, state, and not-for-profit organizations on issues of cybercrime and crimes against children. She may be contacted at susankreston@casec.net.

The author wishes to thank Scott Longo for his contribution to this article.