4-12-2006

A digital forensic practitioner's guide to giving evidence in a court of law

Shayne Sherman
Edith Cowan University

DOI: 10.4225/75/57b1383ac7057
4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 4th 2006.

A digital forensic practitioner's guide to giving evidence in a court of law

Shayne Sherman
School of Computer and Information Science
Edith Cowan University, Perth, Western Australia
ssherma1@student.ecu.edu.au

Abstract

An expert in IT forensics can discover significant and damning evidence that may convict a suspect. However, no matter how momentous the evidence or how clever you may have been at recovering it, if you can't present the evidence in a coherent and understandable way to the court the case may be lost. This paper will attempt to provide you with some translation tools and methods to assist the IT professional in giving comprehensible forensic evidence in a criminal prosecution or at Industrial Relations Commissions to jurors and the judiciary about highly complex IT concepts and recovery methodology. By using these methods, you will have an increased likelihood of your evidence being accepted and understood.

Keywords

Computer Forensics, Digital Evidence, e-crime, investigation.

INTRODUCTION

The extent of computer usage and its natural progression into every facet of humanity has also seen a significant increase in the misuse of this technology for a range of crimes from paedophilia, through fraud to money laundering. This has seen an increase in the need to train more IT professionals in the specific field of computer forensics. Historically criminal investigation using computer forensic skills has been almost the exclusively the domain of police or former police.

Police are provided with, and develop, skills relating to the giving of evidence over many years of exposure to the legal system. However with the increase in demand for computer forensic experts many more people are training as computer forensic professionals, in meeting this demand there is a cost as the vast majority of these individuals have not received training or experience in giving evidence in any jurisdiction. Giving evidence effectively is a skill in itself, the complexity of the methodologies and software currently in use necessities that evidence educed in an analysis should be given in such a way that judge, and juries understand it. There is a duty on anyone who has a high level of knowledge in a particular area that has been tasked with providing expert evidence in a court to provide that evidence in a way that assists the court.

THE DIGITAL FORENSIC PROFESSIONAL AS AN EXPERT WITNESS

What should be apparent to the computer forensic expert, or indeed any serious IT professional, is that they speak another language when it comes to the work they do with computers and technology. How many times when speaking with family and friends are they told not to speak like a "geek" or are asked to "please repeat that, but in words that I understand." Why should the language be seen as anything less confusing when giving evidence in a court before a judge and jury or even talking to the legal counsel that is representing the prosecution or defence?

The work undertaken by the computer forensic expert does happen in a world that has its own language and gizmos. While the last 20 years has seen an exponential increase in people of all ages that have access to computers and who increasingly use them daily on a daily basis does not translate to mean that they understand how they work, or indeed, even want to be able to understand the intricacies of the bits and bytes. The majority of people now see computers as tools and necessities that they need to do many things including work. Similar

to a car most, adults drive and own one but few really know how they work. They just want them to work when they need it to.

By way of example, an IT support person who is working on a help desk and trying to explain why a computer system has frozen or why someone has just lost his or her document. They may as well be speaking in ancient Greek to most people. The thing to remember is that the individuals that contact a help desk are the type of people that may make up a jury in front of whom it may be necessary to give evidence about highly complex computer forensic methodologies and how it has been retrieved information from wiped computers. These same people may have been told more than once "no you have lost that document, there is no way we can get it back".

The possibility that a jury will easily understand something that may have taken the computer forensic professional many years of constant experience and exposure to become familiar is significantly reduced the more complex the issue being explained becomes. This allows the "other side" to be able to undermine the evidence being given regardless of the exacting nature of the analysis that has taken place, resulting in a loss of the case that has been worked on for months or even years in some cases. Chief Judge Dixon suggested, "not only must the expert be speaking on a topic which is an organised branch of knowledge, but it must be capable of application and comprehension by the trier of fact." (Heydon, 2004. p. 940). The observation on experts and their evidence from Dixon CJ in 1960 is as relevant today as it was in the 1960's, which is why it is quoted in the current standard text on evidence of Australian criminal law.

The need to be understood and to understand is beginning to be recognised by the legal profession and courses are now being run for lawyers so that they can understand modern forensic terminology and methodologies. This has not solely been brought about because of computer forensics, but by the use (and some would say misuse) of DNA evidence in legal proceedings. The reason for this is simple, the prosecution and defence are ultimately responsible for ensuring that the evidence educed in court is and can be correctly interpreted or understood by the decision makers, whether it is a judge, jury or both.

It is important to start with a definition of forensic computing, a definition that is generally accepted is that proffered by Rodney McKemmish who said that in his view it is "(t)he process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable." (McKemmish, 1999. p. 1). The concept of forensic computing is a broad one, though this paper will focus on the last part of this definition - "presenting digital evidence in a manner that is legally acceptable". It will however extend to discuss why computer forensic evidence should go beyond being 'legally acceptable' and move to the realm of being 'understood' by the people that need to understand it, the judiciary and the jury.

As a computer forensic professional who may have been requested by the defence or prosecution to provide evidence in a court or commission that person will be regarded as an expert witness. So what does it mean to be an expert witness? A reasonably useful definition is that "(t)he expert witness is an expert in his or her field, and the judge and lawyers are similarly learned experts in theirs. Experts are not in court to argue a case or to expound on the law. Any attempts on their part to do so will quickly produce a ruling from the judge that they are ''Incompetent, Irrelevant and Immaterial'', and rarely if at all will any good come from them." (Jones, 2004, p. 278). This comment by Jones sets one simple rule that should be followed by expert witnesses as he in essence is saying - Stay within your field of knowledge. The danger in a courtroom environment is to stray outside of the field that has been studied or in which a person is expert. This has the potential of placing at jeopardy any and all evidence that has been given by the expert.

The reason for making complex IT forensic evidence understood is highlighted in a recent article on the identified gap in judicial exposure to digital forensics and perception of electronic evidence (Losavio et al, 2006). A survey was conducted in 2005 of 81 judges in Kentucky, USA regarding judicial experiences, expectations and needs for the future in relation to electronic evidence. The preliminary results of the survey conclude, "a gap exists between the preparation of the judiciary for dealing with electronic evidence and expected growth in its use in courts." (Losavio et al, 2006, p.17).

This is further supported in the judicial chain by observations made by Judith Fordham of lawyers in Western Australia soon after she became an Associate Professor in Forensic Science at Murdoch University. In an article in The Australian, dated 11 September 2006 titled "*Lawyers 'don't get' science*" she is quoted as saying that one lawyer wrote to a client about a case, which was largely scientifically based, saying, "(y)ou can't argue with a scientist, we'll have to rely on your character reference". (Lampathakis, 2006). Although this article is particularly focused at scientific and medical evidence the parallels to computer forensic evidence is strong. This places an obligation on the IT forensic professional to 'carry' the lawyer in packaging their evidence in a way that is easily understandable to the jury and at times to the lawyer.

A trap to be aware of is not to over simplify the ability of the jury to comprehend the evidence that is presented. In preliminary findings of another study by Professor Fordham, presented at the International Criminal Law Congress held in Perth in October 2006, she said "her study on how juries dealt with expert evidence showed they were competent at dealing with complex material." ("CSI effect", 2006). The study also "showed jurors wanted more help in trials, including clearer explanations from expert witnesses, more visual aids and the ability to ask questions. They don't just want expert opinion, they want to know how they got there, she said." ("CSI effect", 2006) While the current law does not allow jurors to ask questions, forensic computing professionals can assist with explanations and aids.

When there are complex issues to describe, the saying, "a picture is worth 1000 words" also applies in a court environment. Simplified flow charts and diagrams have been used for many years to explain to judges, lawyers and jurors crimes such as fraud and money laundering. More recently, animations are starting to be used and are gaining acceptance in courts in Australia and the USA.

There are many methods available to assist in making intricate processes more comprehensible, for example, the use of rudimentary PowerPoint presentations can be an effective tool. Use the tools that people who make up a jury are now getting used to seeing and using in their everyday life, slide show presentations, if done right, are not a foreign concept to people in the 21st century. Conceptually people can more easily understand graphics than volumes of complex diatribe by what they perceive as a computer "geek".

Ultimately, it is the responsibility of the lawyer to prove their case or seed doubt in the mind of the jury as the case may be. The role of the computer forensic professional is not to be a lawyer, but to ensure that the lawyer is provided with all the information about the evidence whether it is good or bad, so that they can prepare the case. If graphics are required it is important to liaise with the lawyer and they will make it happen, if they see benefit in it, but be prepared to spend time explaining the evidence in detail to the lawyer first.

When reviewing the literature available on giving evidence as a computer forensic professional it has became apparent that there is very little that addresses how to give this evidence. The overwhelming majority of material covers the seizure, collection, analysis and preservation of digital evidence. Even the US Department of Justice fails to provide adequate direction for investigators after this step and specifically exclude it from their Search and Seizure Manual by stating that "a complete guide to offering computer records in evidence is beyond the scope of this manual" (US Department of Justice, 2002, p. 142).

In Australia the *Guidelines for the management of IT evidence* produced by Standards Australia does not provide practical information on giving evidence that is understood, but refers to the general duty to the court as used in the New South Wales Supreme Court. The general duty is set out in an Expert Witness Code of Conduct appendix (HB 171-2003, p. 31) as:

- An expert witness has an overriding duty to assist the Court impartially on matters relevant to the expert's area of expertise.
- An expert witness's paramount duty is to the Court and not to the person retaining the expert.
- An expert witness is not an advocate for a party.

The 'bible' currently in use by computer forensic professionals is, *A Guide to Forensic Testimony: the Art and Practice of Presenting Testimony as an Expert Technical Witness* by Smith and Brace. The book itself as one

would expect of something written by lawyers is that it almost reads as a legal text with appropriate case law intertwined throughout. The one area that lets the book down is that it does not address methodology of giving expert evidence to a sufficient degree.

Two key chapters relate to giving evidence by telling stories and the role of visual exhibits in expert testimony. (Smith & Brace, 2003). These chapters touch on the possibilities available to simplify complex concepts, however of more use would be a how to guide, as more IT professionals who have not been police officer are becoming more prevalent. The issue of competent ability to give evidence let alone complex IT evidence will be jeopardised if this is not rectified. This will naturally have a knock on effect in the profession with a consequence of clouding the issues when it comes to the courts being confident that a digital forensic expert is just that, an expert.

The Association of Chief Police Officers in the United Kingdom recognises that a good communication skill is a fundamental foundation of independent consulting witness skills. In the *Good Practice Guide for Computer based Electronic Evidence* they state of the skills as being the "ability to express and explain in layman's terms, both verbally and in writing:

- Nature of specialism
- Techniques and equipment used
- Methods of interpretation
- Strengths and weaknesses of evidence
- Alternative explanations" (NHCTU, 2003, p. 31)

AN AIDE MEMOIRE IN GIVING EVIDENCE

In a modification of guidelines for effective testimony (Love, 1995) useful guiding principles for computer forensic professionals giving evidence may look something like this:

- At all times tell the truth
- Understand the ground rules
- Understand the question and don't be afraid to ask for it to be repeated
- Compose a response before answering
- Do not second-guess the questioner
- Do not question or argue
- Be prepared for and withstand harassment
- Do not volunteer answers
- Be attentive and cooperative
- Speak slowly and distinctly
- Correct mistakes – it's okay to make mistakes, it's not okay to not correct them quickly
- Prepare for giving evidence
- Present your own knowledge rather than hearsay
- Refresh your recollection from your statement and logs
- Present your professional judgment

- Interpret photographs, diagrams, processes and reports carefully
- Provide complete but simple explanations with diagrams, if appropriate

In particular, a computer forensic expert should always be prepared to answer reliability questions relating to the software that they have used. This, in a USA context, was brought about by a US Supreme Court decision in assessing reliability in 1995 in *Daubert v. Merrell Dow Pharmaceuticals* and extended to technical evidence in 1999 in *Kumbo Tire Co. v. Carmichael* (Buskirk & Liu, 2006) in which the following four-part test has been established:

1. whether the theory or technique has been reliably tested;
2. whether it has been subjected to peer review;
3. the known or potential rate of error of the theory or technique
4. whether the technique is generally accepted

This type of questioning will become more frequent as the legal profession and judiciary gain more knowledge and become accustomed to computer forensic evidence. Ultimately, all the lawyer for the defence has to do is create a reasonable doubt in the mind of the jury and the defendant could easily be acquitted. A failure to be able to convince the court of the reliability of the software used in any part of the acquisition or analysis of the evidence could raise a reasonable doubt with the resultant dismissal of the expert evidence.

The ability to be able to explain the reliability of forensic computer software, according to the US 'Daubert' test is fundamental to a successful prosecution and fatal if the prosecution has not prepared for this possibility. It is up to the forensic expert to provide this advice or forewarn that this may be an issue and also provide the lawyers with appropriate responses that have previously been accepted in a court of competent jurisdiction.

CONCLUSION

This paper has demonstrated that giving computer forensic evidence in court carries with it a high level of responsibility and expectation. To be effective as a digital forensic professional a person must not only be highly competent when it comes to the capturing, preservation and analysis of computer based evidence. They must also be able to use the most appropriate language or communication strategy to impart the highly complex IT concepts and methodologies in a court so that 'lay' people can make an informed decision. A decision that is not lost in the midst of legal banter about the choice of words, complexity of systems or having to break down the function of each device on a digital system.

The guiding message from this paper is that, as a computer forensic professional do not try to be so quick to demonstrate how clever the evidence has been discovered, that the case is lost because the evidence cannot effectively be communicated to those that make the final decision.

COPYRIGHT

REFERENCES

Buskirk, E.V., & Liu, V.T. (2006). Digital Evidence: Challenging the Presumption of Reliability. *Journal of Digital Forensic Practice.* Vol 1:19-26.

CSI effect impacting on jurors. (2006, October 22). *The Australian*. Retrieved October 26, 2006, from http://www.theaustralian.news.com.au/printpage/0,5942,20626395,00.html

HB 171-2003 (2003). *Guidelines for the management of IT evidence*. Standards Australia. Sydney.

Heydon, J.D. (2004) *Cross on Evidence.* 7th Edition. Butterworths. Chatswood, Australia.

Jones, R. (2004). Your day in court - the role of the expert witness. *Digital Investigation.* Vol.1, p273 - p278. Queen Mary, University of London, Computing Services, Mile End Road, London E1 4NS, United Kingdom

Lampathakis, P. (2006, September 11). Lawyers 'don't get' science'. *The Australian*. Retrieved October 26, 2006, from http://www.theaustralian.news.com.au/printpage/0,5942,20390142,00.html

Losavio, M., Adams. J., & Rogers, M.(2006). Gap Analysis: Judicial Experience and Perception of Electronic Evidence. *Journal of Digital Forensic Practice.* Vol 1:13-17.

Love, T.L. "Guidelines for the witness: pointers for giving effective testimony." *Appraisal Journal* 63.n4 (Oct 1995): 457(8). *Expanded Academic ASAP*. Thomson Gale. Edith Cowan University Library. Retrieved October 29, 2006, from http://0-find.galegroup.com.library.ecu.edu.au:80/itx/infomark.do?&contentSet=IAC-Documents&type=retrieve&tabID=T002&prodId=EAIM&docId=A17783874&source=gale&srcprod=EAIM&userGroupName=cowan&version=1.0

McKemmish, R. (1999). What is Forensic Computing? *Trends and Issues in Crime and Criminal Justice* No. 118. Canberra: Australian Institute of Criminology.

National High Tech Crime Unit. (2003). *Good Practice Guide for Computer based Electronic Evidence*. Association of Chief Police Officers. United Kingdom.

Smith, F.C., & Brace, R.G. (2003). *A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony As An Expert Technical Witness.* Addison−Wesley Publishing Co. Ontario, Canada.

US Department of Justice. (2002). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice. Washington. DC: US Department of Justice.