Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The limits of my tools, my techniques, and myself

With the advance of digital forensic evidence used in legal matters, comes a responsibility to those analyzing and presenting that evidence. It is the responsibility to understand and describe the limits of tools, techniques, technology, and your own capacity.

I often do this when I give talks, and to some extent, it is picking at scabs. Audience members sometimes find it offensive or disconcerting when I point out just how little we know about the things we use in legal situations. In a recent talk on the limits of visualization for forensic purposes, two audience members got particularly unhappy. It may have started when one of them tried to ask an aggressive question that started something to the effect: "In my world, we don't have the luxury of ..." I responded to the presupposition by clarifying that we all work in the same legal world, and that I have to appear in the same courtrooms that they have to appear in, and answer to the same laws and judges. They expressed particular unhappiness about two of my responses. I thought I would share them with you:

> In one case, I pointed out that a file that was supposed to be a forensically sound image was determined to have an extra character at the end of every line that would not normally appear in such a file. They countered that it didn't make any difference since it didn't affect the meaning of any of the content. I tried to explain that an unreliable process could not be relied upon for the rest of the file. After all, if every line had a change we detected, might they also have changes we didn't detect? How can we trust your results if we can't trust your tools? They seemed unconvinced.
>
> In the other case, I was explaining that language such as "match" should be used with a great deal of care, since it implies a far stronger relationship than what we more typically know, which is internal and external consistency or inconsistency. The point made back was, in essence, that the lawyers they work for pay them for their opinions, and often ask them to change meaning to make things more definitive than they really are. I explained that they need to learn how to say "no" politely (or otherwise) and their point was that they won't get the work if they don't shade the facts.

When they left the room, they were pretty outspoken about it (to a third party - they didn't say anything to my face about it.) Of course we all need to consider what we say carefully, and there is a fine line between changes that bring clarity and those that obfuscate.

I have taken to using specific language to describe limits of tools and methods in my reports as part of legal matters. Based on a request that will remain anonymous, I include a sample from such a matter below. It is important to note that I change this for each report I write, depending on the specifics of the situation. And I continue to find a wide range of anomalies and faults in hardware, software, systems, and myself, as I have throughout my career, and as I will likely continue to do for the indefinite future. It is the nature of things.

What might be reasonably said - an example

The National Research Council ["Strengthening Forensic Science in the United States: A Path Forward", 2009, ISBN: 978-0-309-13130-8] recommends that "As a general matter, laboratory reports generated as the result of a scientific analysis should be complete and thorough. They should contain, at minimum, “methods and materials,” “procedures,” “results,” “conclusions,” and, as appropriate, sources and magnitudes of uncertainty in the procedures and conclusions (e.g., levels of confidence)... Forensic reports, and any courtroom testimony stemming from them, must include clear characterizations of the limitations of the analyses, including measures of uncertainty in reported results and associated estimated probabilities where possible." The Reference Manual on Scientific Evidence states "the theory’s testability, whether it was the subject of peer review or publication, its known or potential rate of error, and its general acceptance within the relevant scientific community" [Reference Manual on Scientific Evidence - Second Edition - Federal Judicial Center, 2000]

In carrying out all of these examination, I used an Apple MacBook computer running the OS-X operating system, the Unix "bash" command interpreter, the "Perl" and "Lisp" computer languages, and the programs and mechanisms described herein.

I have found these tools and the methods by which I applied them to be reliable for the purposes discussed and have used and tested these systems, tools, and methods over a period of years to verify that they operate reliably as applied herein. Many of these tools are used on a daily basis in commercial businesses, in government, in educational institutions, and in other settings, by people from all over the world, and they are generally relied upon for the purposes for which they are used in those contexts, many of which are very similar to the uses described herein.

Many of the specific techniques described herein have been published in peer reviewed scientific conferences, and have been accepted within the scientific community to the extent that appearances in peer reviewed publications so indicates.

From a standpoint of identifying possible sources of error and reliability of these tools in this context, I have found that computer programs sometimes produce results that are off by one or otherwise different than what might be attained by hand counts, either because of programming errors that are not detected even after a long period of use, or because of differences in interpretation of what constitutes things like "words", "lines", and so forth.

I have verified each of these results so as to reduce or eliminate such potential errors, and I believe that all of the results herein are accurate as stated.

Summary

I think it is important as a community that we recognize our limitations and our faults so we may best improve ourselves. At the same time, our scientific progress depends on our ability to find ways to reduce these faults and prevent the faults we know about from producing failures that are reasonably preventable. I hope, but don't expect, that everybody working in digital forensics will start to recognize their limitations and use more care and diligence in reporting their findings. And for those who choose not to, I will be looking to help point it out to the other side in your next case...