Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Digital Forensic Evidence: A Wave Starting to Break

Increasingly, legal matters depend on digital information and information systems as the source or repository of the content presented as evidence. With this increased dependence comes a commensurate need to assure that the evidence provided accurately reflects reality. This is the realm of digital forensic evidence (DFE).

As the information age emerges, DFE forms one of the core foci of the legal system. But for such evidence to be admitted in a legal setting, unless it is not based on scientific, technical, or other specialized knowledge, it requires the testimony of experts. In particular, and to more or less quote legal rulings:

- An expert may be qualified by knowledge, skill, experience, training, or education.
- The testimony must be based on sufficient facts or data.
- The testimony must be the product of reliable principles and methods.
- The witness has to apply the principles and methods reliably to the facts of the case.

In the ocean, waves break because the depth of water underneath them becomes too shallow to support the height of the water above. The wave that is starting to break in the legal system is the wave of DFE that has to be presented in keeping with these standards. The reason this wave of DFE is breaking, is that there is not enough depth and volume of expertise to support the volume and complexity of the evidence.

Getting qualified experts

In an emerging field, it's not very easy to get people with many years of experience. While our practice tends to have people with more than 20 years of experience, most practices, and practices with high volumes of cases, simply cannot find people with that much experience, and of course the legal system has not generated enough cases to make for settled law, much less a large cadre of experienced testifying experts.

Knowledge and skill are typically gained by experience, and this means that the most knowledgeable and skilled people are focussed in very specific areas where they have worked for their careers. Finding such experts is a task that is made more difficult by the desire of corporations to keep their employees from working in outside matters and from testifying in legal matters.

Training and education is emerging as a key source of the talent needed to support the legal system. While doctoral level programs in these areas are only starting to emerge today, there are several excellent masters level programs around the world that support digital forensics. These programs are producing perhaps a few hundred people each year who can start their careers and work on the multitude of cases involving evidence identification, collection, and processing.

Getting sufficient facts and data

Attaining sufficient facts and data is the next problem. Most cases within our experience involving DFE are presented with very little evidence compared to the totality of evidence that may be probative with regard to the legal matter at hand. While in simple cases the mere existence of some sequence of bytes may be adequate to resolve the issue, the challenge of attributing actions to actors is a far greater challenge. In a networked environment, the sequence of events leading to a particular situation may involve computers from widely diverse locations containing different fragments of DFE. Identifying, gathering, and analyzing these fragments to form a cohesive picture of what took place is vital to gaining clarity around DFE, particularly when there is the potential for forgery, misidentification, and other similar things. How much is enough? It's a great question, but there is woefully little literature on the answer.

Reliable principles and methods

Processing of evidence has been pretty well defined for simple things, like making forensic images, searching for known strings, and identifying file types by embedded symbol sequences. But in more advanced areas of forensic analysis, such as finding consistencies or inconsistencies between different related items of evidence, associating actions of human actors with event sequences within computers, asserting that a specific sequence of events must have been the cause of the state of affairs when the forensic evidence was gathered, and digital crime scene reconstruction, there is little settled art, few if any standard processes, only limited published principles, and methods are often developed on a case-by-case basis. Worse yet, most forensic "experts" don't apparently calibrate their tools or even know what that means, don't do significant testing of validation, and rely on output from tools whose inner workings they do not understand. Proprietary tools are commonly used and the makers don't revel the details of what they do or how they work. This makes for "secret science" instead of reliable principles and methods.

Applying the principles and methods to the facts

To the extent that there are sound methodologies and well tested and calibrated tools, digital forensics professionals are reasonably good at applying those methodologies and tools to the evidence at hand. But even here, there are no formulaic approaches that work in every case. "Best practice" claims lead to destroying the credibility of a witness. Sound practices are often applied with soundness depending on the reliability of the methods relative to the issues at hand. While many so-called experts make leaps that go too far, careful experts come to similar conclusions when applying the same methods to the same facts.

Conclusions

The digital forensics area is growing in magnitude and intensity, but it lacks in the underlying fundamentals needed to make it viable for legal matters at the volume and intensity they are likely to arise in the coming years. This breaking wave represents both a great challenge and a great opportunity.

