Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

A structure for addressing digital forensics

People that deal with the issues of digital forensics have historically lacked an overarching structure for what the field consists of and how it is carried out. While the bottom-up approach to the technical issues in each of many niche areas has been worked for years, it is sometimes helpful to put these efforts into perspective. Figure 1 shows that perspective as we see it today.

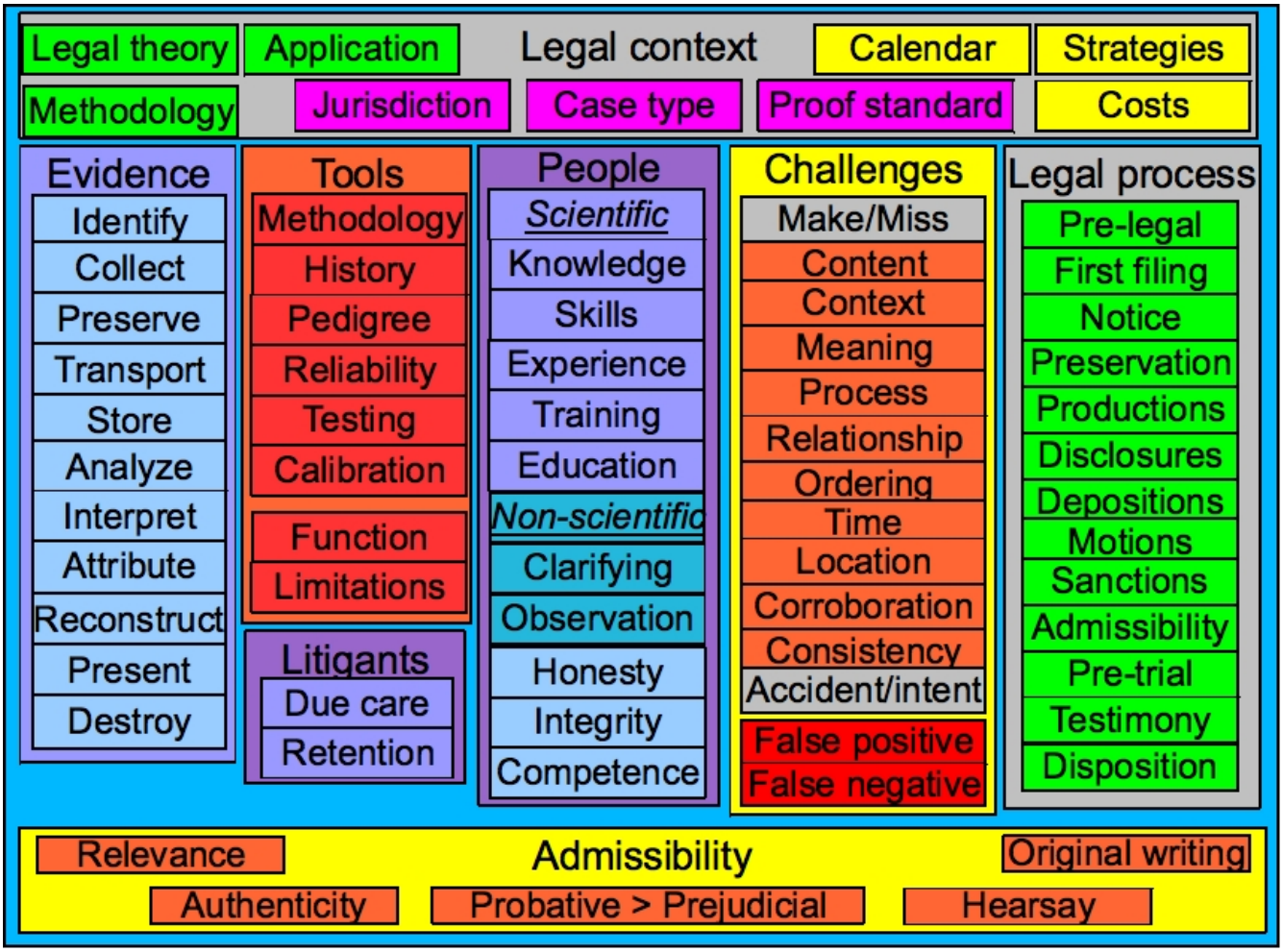

Figure 1 - A structure for addressing digital forensics (see http://all.net/ for drill-down)

Overview of the structure

The structure starts with a legal context, within which the digital forensics expert should act to support or refute legal theories by properly applying established scientific methodologies. This effort is affected by the (1) legal calendar, which forces timeliness and sequencing, (2) legal

strategies, which controls and informs the uses of digital forensic evidence, and (3) costs, which limit the amount of time and effort available to get to the truth. All of this exists within the context of the type of case, the jurisdiction, and the standard of proof associated with them.

Digital forensics experts largely deal with digital forensic evidence and its identification, collection, preservation, transport, storage, analysis, interpretation, attribution, presentation, and destruction. Reconstruction of event sequences may also produce such evidence in cases where that reconstruction can be shown to meet the rigors of the legal system.

To do thus work, forensics experts use tools to allow them and the triers of fact to perceive what is largely, if not entirely, latent evidence, in that it cannot usually be observed by people without such tools. These tools have to be properly applied within the context of a scientific methodology, and have their own history and pedigree that speak to their reliability. They have to be tested and calibrated by the expert if they are to be trusted to produce reliable results, and they have limited functions and those functions and limitations have to be properly understood and addressed in their use. The litigants also use tools and have responsibilities with regard to due care and retention of evidence, and this generally falls into the category of data retention and disposition process and approach.

The expert witnesses that use these tools to provide opinions on evidence have to have adequate scientific knowledge, skills, experience, training, and education to properly apply them using the applicable scientific methodology, and must act honestly with integrity, and competently, if they are to serve justice.

Digital forensic evidence, tools applied to it, and expert witnesses are subject to challenges, and those challenges generally involve the accidental or intentional making of false or missing of content, context, meaning, process, relationships, ordering, timing, location, corroboration, or consistency, that may result in false positives or false negatives with respect to facts or conclusions related to the case.

The legal process may apply digital forensics and experts in that field to aide throughout the case, and when the stakes are high, it may be important to involve these experts throughout the matter to get the best results. From the pre-legal phase, where preparations are underway for a possible legal case, through to the end of the trial and the destruction of evidence per court orders, the skilled digital forensics expert has a vital role to play in assisting legal counsel in their activities.

Summary

That last point, which was also the first point, is indeed worth repetition. Many in the digital forensics field, as in other fields, imagine that they drive the process. In the legal arena, as in most other arenas, technical expertise is only meaningfully applied in the context. The structure described here is useful in tracking and analyzing digital forensic matters within the context of a legal cases. It has been successfully applied to many cases in our practice, and it is available in more depth and with clickable links at http://all.net/ under "Digital Forensics".

