Digital Investigation xxx (2018) 1–5

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Commentary

Accrediting digital forensics: What are the choices?

Keywords:
Accreditation
Certification
Expert evidence
ISO 17025
ISO 17020
ISO 9000
Criminal Procedure Rules

A B S T R A C T

There are three apparent competing routes to providing re-assurance about the quality of digital forensics work: accredit the individual expert, accredit the laboratory and its processes, let the courts test via its procedures. The strengths and weaknesses of each are discussed against the variety of activities within "forensic science". The particular problems of digital forensics, including its complexity and rate of change, are reviewed. It is argued that formal standards may not always be practical or value for money compared with advisory good practice guides.

How do we reassure our customers that they can rely on the expert technical evidence that we produce? Our customers include not only the courts but the investigating agencies, judges and lawyers who commission us. They also include lawyers engaged in civil disputes and in some instances large corporations carrying out internal investigations. We provide evidence that almost by definition a non-specialist audience cannot evaluate for themselves, so that trust is of the essence.

There seem to be three routes: accreditation or certification of those who give evidence, accreditation of the laboratories and processes upon which they may depend, and reliance on testing via court procedure and cross examination. Each have strengths and weaknesses. Whichever we choose, though, has to be both practical in terms of implementation and financially viable in terms of delivering value for money.

The issue of method of accreditation is not wholly theoretical and academic. The authorities both in the United States and in the United Kingdom, among others, are seeking arrangements by which non-certified individuals and laboratories may be denied contracts or may even be forbidden from giving evidence in court.[1] Although the advantages of such policies seem obvious there are also drawbacks if schemes are clumsily conceived. This is particularly true for digital forensics.

Individual accreditation

The accreditation/certification of an individual depends partly on their qualifications and partly on their experience. Any scheme, if it is to have credibility, must be based on objective criteria. It would be unfortunate if accreditation depended solely on friendship with a self-appointing self-perpetuating collection of experts. Awkward decisions have to be made about the governance of such a scheme; it needs credibility itself. It would also be unfortunate if there were a multiplicity of rival accrediting organisations.

What would the criteria actually be? In the digital forensics field there are any number of post nominals available. Some will be degrees from recognised universities, others from voluntary and commercial training organisations and yet others signify no more than that someone has taken a training course in one specific analytic product and been presented with an extravagantly printed certificate at the end. In all cases much will depend on the syllabus under which the qualification was obtained, how up-to-date it is and how far there have been refresher courses to cope with the ever-changing digital landscape. How is one to measure experience? Will a mere recital of lists of cases be sufficient or will it be necessary to consider a collection of actual reports? Where do you get your assessors from? In the scheme once used in the United Kingdom a selection of reports was read by assessors against a list of desirable criteria to demonstrate skill. Qualifications had to be "proved" by the production of appropriate certificates and statements from referees were also required. The UK scheme, which aimed to cover all forms of forensic science activity, was abandoned because its government sponsor had hoped that it would become self-funding, which it never did. Neither did it help that applications for registration were voluntary.[2] Many of the concepts though live on in arrangements used by the Dutch judicial system (https://english.nrgd.nl/).

Laboratory accreditation

The accreditation of laboratories and processes seems to offer fewer practical problems of implementation. The chosen international standard is ISO 17025. This standard specifies the general requirements for the competence for laboratories to carry out tests

[1] https://www.justice.gov/archives/ncfs/page/file/624026/download; https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674761/FSRAnnual_Report_2017_v1_01.pdf.

[2] http://www.computerevidence.co.uk/Papers/ComputersandLaw/RegisteredForensicPractitioner.htm; http://library.college.police.uk/docs/homeoffice/Review-of-Forensic-Practiti1.pdf.

https://doi.org/10.1016/j.diin.2018.04.004

and/or calibrations, including sampling. It covers testing and calibration performed using standard methods, non-standard methods, and laboratory-developed methods. It is not specific to forensic science. It seems to work well for traditional "wet" forensic science laboratories which carry out series of individual tests on DNA, blood, fibre, fingerprints and paint fragments. Senior forensic scientists will have researched the underlying science and arranged for it to be written up in a peer-reviewed journal; they will have designed tests which incorporate the science but also cover the management aspects of practical forensics – to include recording and reporting. Once established, commoditised routine work can be passed on to forensic technicians. The overall process needs "validation". For each process what is required is a statement of end-user requirements, a formal specification, a risk assessment indicating the potential limits of the value of the process, a formal statement of the acceptance criteria, a formal validation plan followed by an exercise and assessment followed by a report supported if necessary by a library of results. All this must be properly documented. At the end of the process there is a statement of validation completion. Assessment is carried out by a third party. This is the scheme currently promoted by the U.K.'s Forensic Science Regulator.[3]

There has been some discussion of the possibility of producing a standard for the evaluation of evidence[4] though this has concentrated mostly on problems associated with statistics.[5] Another proposal under consideration is trying to find a standard for "case review" which would cover the work of defence experts.[6] The proposed standard is ISO 17020 which in its original design specifies requirements for the competence of bodies performing inspection and for the impartiality and consistency of their inspection activities. But there are grounds for wondering what an assessment on these bases would look like and whether the issues are better tested via court procedure.

Court procedures

Testing via court procedure can obviously only take place either at trial or shortly before. Some countries follow variants on the US practice of making novel scientific evidence an issue of admissibility with the judge acting as a gate-keeper against "junk science". It follows the so-called *Daubert* tests[7] to demonstrate that a method is generally accepted by the scientific community: that a theory or technique is falsifiable, refutable and testable, has been subject to peer review and publication, and that there is a known or potential error rate. The UK adopts these broad ideas, but within the discretion of a judge, via the Criminal Practice Directions 19A 3–6.[8]

In many jurisdictions there will be codes of practice or regulations governing the presentation of expert evidence. Among these will be requirements for the contents of an expert report. Typical elements will include: a statement of an expert qualifications, the instructions given to the expert, a list of material considered (which might include exhibits seized by others but also reference material and literature), extent of dependence on others, investigations carried out, results, analyses of alternative hypotheses, and conclusions.[9] An obvious implicit requirement is that a suitably qualified expert hired by "the other side" should be able to follow each step and carry out their own tests.[10] The actual circumstances will vary between jurisdictions. For example where the criminal procedure is accusatorial (as is the case in procedures based on the English common law and widely used in countries formerly part of the British Empire) a prosecution expert report will be made available before trial to a defence expert and there may be discussions to identify points of agreement and disagreement prior to trial start. In courts based on the European code system the procedure is inquisitorial where much of the investigation is managed by a judge as opposed to the police by themselves. The judge will want to have access to an expert and it will only be at trial that the expert's work is tested. In both cases, however, what is actually eventually happening is detailed peer review by a defence expert of the work carried out by the prosecution expert. In effect this testing can only take place if the respective experts with their appropriate levels of competence can be identified – which brings us back to how we accredit the individual. Much may also depend on the skills and knowledge of the presiding judge.

Variety of "forensic science"

One of the questions one must ask is whether a single scheme of accreditation works across the entire range of activities within forensic science. In addition to the series of commoditised single purpose tests envisaged within ISO 17025 expert evidence can also rely heavily on the experience of an individual. This is particularly true of psychiatric and psychological evaluations where there is seldom much in physical form to be tested; if there is doubt about the evaluation of one psychiatrist then the usual route is simply to call in another qualified medical professional and give them the opportunity to interview and look at the life history of the subject. But it is also true that many experts are required to carry out reconstructions of events; typical instances could involve road traffic accidents and murder scenes. The forensic scientist will have physical evidence to examine and will need to carry out a series of tests on each element but the actual reconstruction requires experience. An expert report will need to spell out all the elements involved in reaching a particular reconstruction and it will need to have sufficient detail so that another expert can agree or disagree. A properly written report will look at alternative hypotheses and perhaps assign percentage probabilities to any favoured interpretation.

The importance of separating a technical investigation and evaluating its implications was discussed in a recent editorial in *Digital Investigation*.[11] ENFSI has a publication *Guideline for Evaluative Reporting in Forensic Science*.[12] OSAC's publication *A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence*[13] has a useful chapter on reasoning in forensic science and distinguishes between abductive, deductive and inductive reasoning. "Abductive reasoning eliminates implausible explanations and retains the most plausible explanation for (limited) available facts and traces, drawing analogies from past experience.

[3] https://www.gov.uk/government/organisations/forensic-science-regulator.

[4] https://doi.org/10.1080/00450618.2013.784361.

[5] See also: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/674761/FSRAnnual_Report_2017_v1_01.pdf, paragraph 1.2.

[6] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/674761/FSRAnnual_Report_2017_v1_01.pdf at paragraph 1.13.

[7] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 US. 579 (1993).

[8] https://www.justice.gov.uk/courts/procedure-rules/criminal/practice-direction/2015/crim-practice-directions-V-evidence-2015.pdf.

[9] See the UK rules in CPR 19.4 (https://www.justice.gov.uk/courts/procedure-rules/criminal/docs/2015/crim-proc-rules-2015-part-19.pdf and the US Federal Rules 703 and 704.

[10] See for example Principle 3 in the ACPO Guide to computer-based electronic evidence: "An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result".

[11] Digital Investigation 19 (2016) A1eA; 3 https://doi.org/10.1016/j.diin.2016.11.001.

[12] http://enfsi.eu/wp-content/uploads/2016/09/m1_guideline.pdf.

[13] https://www.nist.gov/sites/default/files/documents/2018/01/10/osac_ts_0002.pdf.

Please cite this article in press as: Sommer, P., Accrediting digital forensics: What are the choices?, Digital Investigation (2018), https://doi.org/10.1016/j.diin.2018.04.004