Accrediting digital forensics: what are the choices?

Peter Sommer

peter@pmsommer.com; peter.sommer@bcu.ac.uk

This is a preprint of article to appear in Digital Investigation *journal (https://www.journals.elsevier.com/digital-investigation) as DIIN756; https://doi.org/10.1016/j.diin.2018.04.004https://doi.org/10.1016/j.diin.2018.04.004; if citing please refer to final published version*

Summary:

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.

Keywords:

accreditation, certification, expert evidence, ISO 17025, ISO 17020, ISO 9000, criminal procedure rules

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[i]. 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[ii]. 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 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 UK's Forensic Science Regulator[iii].

There has been some discussion of the possibility of producing a standard for the evaluation of evidence[iv] though this has concentrated mostly on problems associated with statistics.[v] Another proposal under consideration is trying to find a standard for "case review" which would cover the work of defence experts[vi]. 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[vii] 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[viii].

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[ix]. 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[x]. 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*[xi]. ENFSI has a publication *Guideline for Evaluative Reporting in Forensic Science*[xii]. OSAC's publication *A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence*[xiii] 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. Deductive reasoning tests this most plausible explanation against observable traces, possibly through further study of facts, with particular scrutiny for contradictory facts (falsification). If any contradictory traces are found, the most plausible explanation must be revised. Inductive reasoning can lead to knowledge specific to an event or a case, providing decision-makers with trustworthy understanding of the traces to help them make decisions. Inductive reasoning can also lead to a theory generalized from multiple cases or from repeatable experiments, providing newly established knowledge in forensic science."

What is special about digital forensics?

Digital forensics has some special qualities which do not fit easily into any of these accreditation plans. Most digital devices are akin to a whole scene of crime. There will be a large number of potential artefacts and different requirements of how they are to be handled. In the simplest of situations all that may be needed is to show that a particular file is present. But often what is also expected is an account of how that file arrived on that device – and what inferences one might draw as a consequence. A file might have been generated by the owner of the computer, it could have arrived as an email or email attachment, via social media, via web browsing, via file sharing. A prosecution case may need to be built up not just on the basis of one file but of a sequence of events – successive use of web browsing, sequences of emails and social media postings and so on. An expert may be invited to draw conclusions about a subject's courses of action, research and what can be inferred about intent. And this is on the assumption that the files of interest are all extant and that no data recovery of deleted material is called for.

A second feature is rate of change: hardware, operating systems, and application programs are constantly being updated. As a result, software tools can become rapidly obsolete. I sought to deal with the implications of this back in 2009 in an article *Forensic Science Standards in Fast-Changing Environments*[xiv]. If anything, the problem has become more acute as rates of change have speeded up; smart phone apps may be "updated" as often as every two weeks. The essential problem is that the speed of change is much faster than the rate at which an artefact with evidentiary potential can be identified and analysed, written up in a peer reviewed journal article, published and then made the subject of a reliable tool – which itself would then need to be validated.

Then there is the problem of examinations which are "one off", or at least that is how things start. This is particularly true of the increasing number of circumstances where hardware must be examined; examples include "off chip" and JTAG physical examinations, IOT devices and devices associated with automatic teller machines and point-of-sale systems. But it can also be true when a new app, messaging service or social medium appears and very quickly acquires large numbers of followers. Often these issues arise because there is an immediate investigative requirement – what

is the law enforcement officer to do if he is told that there is no current approved forensic technique?

Another issue raised in the same article has also become more acute. In practice most digital forensic examinations use not single purpose tools but integrated analysis suites which offer, among other things, safe forensic imaging of original devices, automated recovery of deleted files, a series of viewing environments for the contents of the devices, complex searches, facilities to extract material to produce exhibits, and the automated generation of reports. Without such integrated tools productivity would drop near to zero. Almost no computer investigations would be completed at timescales acceptable to the courts – or indeed to the public; already in the UK non-urgent computer and phone examinations by law enforcement may have waiting lists of over six months. What is relatively new has been the appearance of "evidence finder" type products aimed at providing many examination facilities for the less skilled. Smart phone examinations, of the limited sort, can be carried out on "kiosks"[xv]. These products offer results at lower costs and higher speed of delivery than the more traditional suites which require greater levels of technical knowledge and need more training. But how do you apply testing of the sort envisaged in ISO17025, particularly when the products themselves are, as they must be, subject to frequent updating?

Problems of standards

In the 2009 article I wrote: "Where this leaves us is that if current proposals for certifying the output of forensic science labs and tests for the admissibility of scientific evidence are enacted strictly large sections of computer-related evidence will either not be allowed to emerge from the labs or be ruled inadmissible by the courts. Digital evidence will have to be at least a year perhaps more behind the ways in which computers are used by organizations and individuals – and criminals." This is a particular problem in the US if the *Daubert* tests are strictly applied. A further problem with *Daubert* and indeed ISO 17025 is the emphasis on "error rates" associated with a particular tool or method. In the context of much traditional "wet" forensic procedures error rates are important, the more so if they can point to probabilities and "likelihood of evidence". But here too there is a poor fit with the digital forensics, a matter discussed interestingly and at length by the Scientific Working Group on Digital Evidence in its publication "*Establishing Confidence in Digital Forensic Results by Error Mitigation Analysis*"[xvi] in which the authors list out the types of errors that can occur and show how few of them lend themselves to estimates of rates of error. "The primary limitation of testing is that no amount of testing can prove that the tool is functioning correctly in all instances of its use. Even if all tests produce the expected results, a new test scenario could reveal unexpected results. "

One of the problems with standards is a tendency to bloat. This is particularly true of those that have moved beyond the original aims behind standards, which was that if screws and other mechanical objects were being manufactured by several companies they should all work together and also that they featured quality sufficient for the tasks they being asked to perform, for example not fracturing prematurely and allowing users to work with them safely[xvii].

The people charged with developing the more abstract type of standard seem to keep adding features – and boxes to be ticked – because they believe that the greater the level of detail the "better" the standard is. But standards are not an end in themselves; they come into existence because it is hoped that there are wrongs that can somehow be corrected. The ever-increasing world of standards committees can become detached and self-referential. They run the danger of forgetting why they exist. Compliance with standards costs not only in requiring change in business processes and in demanding extensive documentation but in paying the independent assessors.[xviii] In the end there has to be a value for money test measured against how far the identified wrongs are

being corrected. Most of forensic science is paid for from public funds gathered via taxation. This is true whether the direct purchaser is a law enforcement agency, a prosecutor, a judge or a defence lawyer.

Those who have complained about standards "bloat" can find themselves accused of not caring sufficiently about "quality" or being told that the job of a standards body is about excellence and that costs are a policy problem for someone else. It is instructive to look at the standards relating to information/cyber security. The standards now adopted originated in the mid-1990s in the United Kingdom through what was then called BS 7799. The modern form is the ISO 27000 series. It has become very expensive to adopt in its complete form so much so that only very large organisations can afford it. However instead of insisting on compliance and saying that those who fail should not be allowed to operate or forbidden certain types of contract. NCSC/GCHQ evolved a program called Cyber Essentials, the aim of which is reasonably clear from its name[xix]. In effect is exists in two forms, the lower involves self certification and a higher external certification. This pragmatic approach achieves many of the aims of having regulation/guidance in the first place without disproportionate expense[xx].

Throughout this debate about quality the issue of cost is often forgotten. A survey carried out in the UK in 2017 reported costs to achieve ISO 17025 of tens of thousands of pounds sterling[xxi]; many respondents described the costs as disproportionate particularly as the prosecution and legal aid authorities were, as part of broader government economic policy, seeking to reduce fees for substantive work – from which the assessment costs would have to come. But of course, the people who do the assessment need to be paid – and the greater the level of detail required from them the larger the fee they will require. One of the many reasons why the earlier UK scheme for registration of forensic practitioners failed was that assessors had to be drawn from the ranks of highly experienced technicians/investigators but were only paid £40 ($50) for each assessment; but there was also resistance from candidates who felt that even the £165 fee was too much; no wonder initial enthusiasm rapidly evaporated.

Solutions?

How do we take this forward? Part of the problem is that too much of the public policy discussion about improvements to the provision of expert evidence to the courts has proceeded on the basis that the entire issue is "forensic science" as opposed to the other roles of the expert, which as we have seen, can involve evaluation and interpretation of ambiguous results, reconstruction of events, and the provision of background information about particular commercial practices, technologies and socio-cultural phenomena. It is also worth remembering that the function of the courts is, in criminal cases, to see if a prosecutor has assembled enough evidence to persuade that there should be a conviction under a specific statute or common law, and, in civil cases, to reach a conclusion in a dispute between citizens. Science is an assistance in this process, not a determinant nor is it a role of the courts explicitly to decide on "science".

The conclusion must be that, however one may wish it otherwise, there is no single "one size fits all" route to assuring quality in digital forensics evidence and it is a mistake to try and force any one solution. The ISO 17025 route to certifying processes looks as though it will struggle once one moves beyond the simple tasks of evidence acquisition and preservation[xxii]; even here although the situation is stable for hard disk acquisition matters are less clear given the ever-hardening protections on access to smart phones, the increasing requirement for evidence from social media

and the variety of cloud storage. Many practitioners also point out that ISO 17025 refers to laboratory processes and that, since for the most part they are working on forensic image copies and not originals, much of digital forensics is not conducted in anything that can properly be described as a laboratory.

But peer review of an expert report by an opposing expert implies the existence of a cadre of reliable people willing and able to carry out the work – and there are few national standards and no firm international standards for accrediting them.

Let's return to the question at the beginning of this article. How do we reassure our customers that they can rely on the expert technical evidence that we produce? Given the special qualities of digital evidence, that individual devices usually contain many different potential artefacts, that interpretation of a crime scene is often required and the speed of technological change, we need to recognise that the aim of bureaucratic simplicity – "here is the one type of accreditation to look for and you will be able to rely on the results" – is alas doomed to disappointment. That, or a rigid system which will result in many forms of plausible evidence being denied the courts and with the result that criminals go free.

We will have to make do with a rather messy combination of tests for reliability. ISO 17025, ISO 9000 and ISO 27037 have benefits for accrediting digital evidence acquisition and preservation. It is however interesting to note that ISO 17025 does not provide an absolute guarantee of quality. At the time of writing the UK scheme is faced with two major problems associated with companies that were registered, though neither operated in the digital domain. One has former employees facing criminal charges involving data manipulation[xxiii] and another failed financially leaving the police to have to fund substantial amounts of retesting[xxiv].

In terms of accrediting individuals, it would probably pay national governments to invest in schemes to which they are willing to give authority; it may be that they could rely heavily on piggybacking on selected existing certification and accreditation schemes. Perhaps an advisory board could identify worthwhile qualifications to guide prospective customers and the courts – while stressing the importance of seeking evidence for continuing professional development.

A further useful solution can consist in the creation of detailed *Good Practice* guidance[xxv], as opposed to mandated standards, which can then be applied in specific cases on a discretionary basis by judges and after hearing arguments from lawyers and experts. In the UK there is a bill currently before Parliament setting up a forensic science regulator on a statutory basis and charged with producing a code of practice[xxvi]. Although the regulator would have powers to investigate, breaches of the code would not automatically incur criminal or civil liability; but the courts would plainly bear such breach in mind. Much will depend on what any code of practice actually says. The forensic science regulator is also currently seeking arrangements by which if an expert is criticised by a judge that criticism is made available widely to judges and those who commission forensic science activity[xxvii].

There is no doubt that this mixed approach lacks the clarity and simplicity many people desire but in striking a balance between the problems of achieving a "pure" scientific approach to accrediting forensics and the need to see that the courts can cope with the latest in cybercrime and cyber breach activity we must remember that the administration of justice has always needed strong

pragmatic qualities. And for customers seeking digital forensics expertise there is also the important additional route of seeking informed informal recommendations from others.

Note: In addition to his practical, public policy, and academic work the author was the joint lead assessor at the UK's Council for the Registration of Forensic Practitioners, served on the Digital Forensics Specialist Group of the UK Forensic Science Regulator, and advised the Netherland Register of Court Experts (NRGD), SWGDE, and ISC²in its testing of CCFP. The author thanks Eoghan Casey for comments on an earlier draft.

---

[i] 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

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

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

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

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

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

[vii] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993)

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

[ix] 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.

[x] 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."

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

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

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

[xiv] https://doi.org/10.1016/j.scijus.2009.11.006

[xv] Eg https://www.msab.com/training/kiosk/

[xvi] https://www.swgde.org/documents/Current%20Documents/SWGDE%20Establishing%20Confidence%20in%20Digital%20Forensic%20Results%20by%20Error%20Mitigation%20Analysis

[xvii] http://arussell.org/papers/futuregeneration-russell.pdf; https://www.ansi.org/consumer_affairs/history_standards

[xviii] See criticism of the ISO 9000 quality series, eg https://www.sciencedirect.com/sdfe/pdf/download/eid/1-s2.0-S0007681301800343/first-page-pdf; http://asq.org/learn-about-quality/iso-9000/overview/is-it-worth-it/iso-9000-ineffective.html; https://link.springer.com/article/10.1023/A:1018591430752

[xix] https://www.cyberessentials.ncsc.gov.uk/

[xx] Similar criticisms over costs and relevance were made of US computer security standards TCSEC and its successor Common Criteria for failures to certify in a timely fashion the operating systems that were at any time currently in use as opposed to ones one or two generations old.

[xxi] http://digital-evidence.expert/UK%20ISO%2017025%20Digital%20Forensics%20Survey%20April%202017.pdf

[xxii] in any event there is a separate existing standard for the identification, collection, acquisition and preservation of digital evidence – ISO 27037

[xxiii] http://www.independent.co.uk/news/uk/crime/forensic-labs-data-manipulation-criminal-convictions-doubt-randox-testing-services-investigation-a8066966.html

[xxiv] https://www.thetimes.co.uk/article/police-foot-the-bill-after-collapse-of-forensics-firm-key-forensic-services-limited-bg5nbxkxt

[xxv] http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf; http://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf; https://vault.fbi.gov/digital-evidence-policy-guide

[xxvi] https://services.parliament.uk/bills/2017-19/forensicscienceregulator/documents.html. Note: this is a private member's bill, which means it does not currently have government backing and may therefore not succeed.

[xxvii] https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/2018-03-16-Letter-from-Science-Regulator.pdf