Forensic science standards in fast-changing environments

Forensic Science Standards in Fast-Changing Environments

Peter Sommer

London School of Economics & Political Science, Open University, UK

Abstract: *Regulatory trends in forensic science point strongly to the need for exhaustive testing of all findings and tools. At the same time a number of jurisdictions suggest a judicial test for the admissibility of novel scientific evidence. But in fields such computers and cellphones, the rate of change is faster than the normal times required for peer-reviewed publication. One route to admitting less-than-perfect findings from forensic science is via a re-evaluation of the role of expert evidence and in particular pre-trial meetings between experts.*

This paper is based on a presentation Keeping Up: Testing Methodologies in Digital Forensics *given at EAFS 2009 in September 2009. It will appear in a forthcoming edition of* Science and Justice. *Please treat this as a pre-publication version and check with the final version in the journal.*

The message from forensic science to expert witnesses is clear: evidence tendered should be based on validated scientific knowledge; all tools and procedures deployed should have been subject to independent testing to demonstrate compliance with their stated claims.

But the establishing and validation of scientific knowledge takes time. Even when the particular element is simply a modest refinement of what was already well-known, suitably exhaustive tests have to be carried out, a paper has to be prepared, this in turn has to be subjected to peer-review and then published, hopefully in the next edition of a relevant journal. It is only at this point that an associated practical procedure can be devised and, if helpful, tools designed. And then these too have to be tested and, ideally, the test results published and a certificate of some sort issued.

What happens if the raw material with which you work changes at a rate faster than these cycles of publishing and testing? There have been many improvements in the handling and analysis of DNA (RFLP, PCR, STR, AmpFLP, Y-chromosome, Mitochondrial) since Alec Jeffery's paper in 1984 indicated its value as a unique marker of identity, but DNA itself has remained unaltered. Methods of analysing and identifying paint fragments have also undergone a variety of developments over the years, but the appearance of brand new paint technologies (changes in pigments, binders, solvents, additives) which cannot be incorporated into the existing range of analytic techniques are extremely rare.

This is not the situation with evidence derived from computers where the extraordinary rates of change in Information and Communication Technologies (ICT), the very wide usage of communications networks, and the socio-cultural-commercial environments which are thereby made possible, are all reflected in activities carried out by practitioners in digital forensics.

Expert evidence around computer-related activities ought to meet the same verification standards as the rest of forensic science, but in practice the vast majority of it doesn't and it is difficult to forecast a point at which it ever will - or indeed envisage the process by which this might happen.

This creates the dilemma which I wish to explore: if we insist on very high standards for the verification for scientific and technical evidence methodologies we run the risk of excluding material, particularly if it is digital in form, which might assist a court in reaching a conclusion; we could easily be letting the guilty go free. On the other hand, without rigour, we open the courts to becoming confused by junk science. The answer, I suggest, is a re-siting of forensic science within the broader duties of the expert witness and looking at how existing features of the criminal procedure rules might be exploited or modified.

Forensic Science standards for verification

Proposals now in train seek potentially to embed the notion of exhaustive verification and testing into the forensic process, and to exclude any scientific and technical evidence which fails these criteria.

The Law Commission's Consultation Paper No 190 *The Admissibility of Expert Evidence in Criminal Proceedings in England and Wales: a new approach to evidentiary reliability*[1] makes a provisional recommendation for a statutory test to determine the admissibility of expert evidence. The test would exclude evidence unless it was "sufficiently reliable" and that in turn would be tested against a statutory list of guidelines. One of the suggested guidelines would be a variant of the US *Frye* test[2] of proof of "scientific acceptability" or the more specific *Daubert* tests[3] which include publication in a peer-reviewed journal.[4] The rules appear in Table 1. It would be for the person hoping to tender expert evidence to show the judge that his/her work met the criteria for reliability. Even if "publication in a peer-reviewed journal" is simply regarded as a guideline and is not mandatory, as few judges are likely to be have much background knowledge of the many sub-disciplines within forensic science, one can foresee a situation when the journal article criterion becomes quasi-compulsory.

---

[1] http://www.lawcom.gov.uk/docs/cp190.pdf

[2] 293 F 10113 (1923)

[3] 509 US 579 (1993)

[4] The Law Commission considered four possible options: exclusionary discretion without guidance, exclusionary discretion with guidance, an admissibility test requiring consensus amongst experts in the field; an admissibility rule requiring the trial judge to assess the evidentiary reliability of tendered evidence (para 4.3). This last is close to the *Daubert* type of approach and finds greatest favour with the Law Commission (Parts 5 and 6)

A second arena demanding very high levels of validation and testing is forensic science regulation. The UK Forensic Science Regulator has been in post since February 2008; the role is to identify and develop quality standards among those providing forensic science services. [5] One of the key documents is to be called *Quality Standards for Forensic Science Services*. It is still being formulated but a good idea of the approach can be seen from its *Version B*[6] which closed for comment in May 2009. Section 14 deals with "Development, validation, verification and implementation of new methods, products and services". Section 14.3.5 deals with "validation" and 14.3.5.2 with "objective methods": "For a full validation of an objective method, the provider shall systematically assess all the functional and performance requirements and the parameters/characteristics that are capable of influencing the result and are relevant to the intended use." In relation to products that are to deployed, the document says: "The functional and performance requirements of a product shall address its reliability to deliver consistent and reliable results in the range of circumstances in which it might be applied or used." And section 15.3.5.4.1 extends this to software unless it is commercial off-the-shelf and in widespread general use. In all instances a validation report is required.
There is a linked expectation that forensic science laboratories will comply with the ISO/IEC 17025:2005 standard which specifies the general requirements for the competence 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[7] and also places great stress on the exhaustive validation of methods and tools. ISO/IEC 17025:2005 itself is based around the ISO 9000 series of quality standards.

Computer Forensics

The importance of the disciplines associated with the identification, acquisition and analysis of material from computers can be gauged by the following: By 2008 70% of UK homes had at least one personal computer and of those 93% had a broadband always-on connection to the Internet. [8] Costs of data storage (hard-disks) halve every 18 months or so.[9] A "reasonable entry-level" but actually very powerful personal computer can be bought on the High Street for 3 days' earnings of the average worker. Broadband brings much greater speeds and hence much more data per second and the monthly flat rate frees the user from the need to economise in Internet sessions. There are several multipliers in place: more time online, more data downloaded, cheaper personal computers with cheaper data storage has enabled experimenters and entrepreneurs to launch new data-intensive services such as social networking, media downloads, more extensive e-commerce sites, more complex and sophisticated e-banking and other financial services sites.

---

[5] http://police.homeoffice.gov.uk/operational-policing/forensic-science-regulator/about-the-regulator/

[6] http://police.homeoffice.gov.uk/publications/operational-policing/Quality_Standards_for_FSSPs1.pdf?view=Binary

[7] http://www.iso.org/iso/Catalogue_detail?csnumber=39883

[8] Ofcom: *The Consumer Experience 2008 Research Report*

[9] In 2004 the cost per megabyte of a hard-disk was $1.15; in 2009 (at the time of writing) it is 5-6 cents. Then 250GB was thought huge; today 1500 GB disks cost about $100.

More material downloaded and stored, and now accumulated over longer periods means more "digital footprints".

As a result, whilst in the early days of forensic computing the pre-occupations were "hacking" and "computer fraud", today there are very few crimes where evidence from computers does not potentially play a role.

In practice there are fewer than 100 prosecutions per year under the Computer Misuse Act 1990, largely because the Crown Prosecution Service prefers to use what it regards as substantive statutory routes as opposed to those that refer to the *modus operandi*. Thus most "computer fraud" is handled under the Fraud Act 2006, s 2(5) of which specifically refers to the use of computers. There are now several varieties of fraud which only exist because of the way in which the Internet has developed – "phishing", e-commerce and auction frauds are obvious examples. Other areas where evidence from computers has been important include: child sex abuse, murder, terrorism, software and other IP piracy, money laundering, people trafficking, narcotics importation and trafficking, handling stolen goods, harassment, sexual assault, electoral abuse, perjury, attempts to pervert the course of justice, and police disciplinary proceedings.[10] Often what counts is when the evidence is corroborative and indicative rather than directly supportive of an allegation: very important sources are emails and Internet searches. In terrorism cases the material may include downloaded bomb-making manuals. The 2003 Criminal Justice Act permits prosecutors to apply to be allowed to admit so-called "bad character" evidence[11] and computers may be a rich location for this by, for example, showing patterns of visits to certain websites.

Computer forensics became a nascent discipline at the end of the 1980s. Up till then, "computer evidence" had usually meant "computer print-out" – a paper-based selection from a database or set of documents held on a mainframe. But the arrival of the personal computer, one that was not solely for the use of hobbyists and moreover a machine that had hard-disk storage, changed all that. Mainframe computers cannot be readily seized, PCs can. An entire hard-disk can be copied / cloned and then analysed. This is still one of the core jobs within computer forensics, though capture and analysis of network traffic and the examination of devices such as cellphones, PDAs, digital cameras and portable media devices are also important as well.

Examining a hard disk is not limited to simply looking for "killer fact" substantive files. Files acquire a variety of date/time stamps from which chronologies can be built. Modern operating systems have areas which contain configuration detail which speak to how a computer has been set up and used. They have a variety of features to ease the user experience (such as remembering certain bits of information or caching activity) and to increase resilience to cope with failures. More modern operating systems also take snapshots of the computer at regular intervals and create full text indexes of the disk contents. Data that is deleted does not disappear immediately but is merely *marked* as deleted, so that many forms of data recovery are possible.

---

[10] These are all from the author's own case book of instructions

[11] Criminal Justice Act 2002 Part 11Chapter 1 ss 98-107

Speed of Change

But the ways in which they achieve these facilities change with each new version of an operating system; whilst the regular user of a computer simply notices the new graphics of the user interface and the changed menu items, what is going on under the hood changes dramatically as well. Consider Table 2 – this is a highly simplified history of the family of operating systems used on over 90% of PCs. Looking simply at the differences between Windows XP and its successor Vista: many of the basic locations for critical files were changed, there were new file and disk back-up facilities, new ways of recording time and date stamps, in-built disk indexing, a substantially changed system for email storage, and many other alterations and new features too extensive and complex to list here[12]. The table, in its highly abbreviated form, significantly under-states the frequency of change. Individual versions of operating systems are also the subjects of updating – there have been three "Service Packs" for Windows XP, for example. But beyond these, as most Windows users know only too well, minor updates are provided *once a week*. When these updates occur, although there is often some explanation of what they are supposed to offer, the ways in which they do so are usually highly opaque.

However, this is just the changes to operating systems. Over the same period, since 1984, there have been important developments in the way in which hard-disks are designed and how they interface, physically and logically, to a computer. Without an understanding of these changes, any device which claims to be able to make a complete copy of hard-disk, so-called forensic disk imaging, may fail to capture all the data that is available.[13]

More immediately visible to most users are the application programs. Although even something as familiar as a word processor appears to be relatively unchanging over the years (see Table 3), each new version has features which might be turned to forensic use. Microsoft Word can trace its history back to 1983 and Word for Windows to 1989. Over the years newer versions have developed "undo" editing facilities which can result in deleted material being recoverable and "properties" which retain information about where and when a document was originated as well as successive versions. But subsequent versions of Word create more "hidden" information and different types of "properties" or "metadata" information.

But many of the most common and popular applications have been in existence for far shorter periods. The function of a web browser is to enable the retrieving, presenting and examination of information on the world wide web (www). The idea behind the world wide web dates from 1991. Microsoft's Internet Explorer, now at Version 8, appeared in 1995 but took some time to gain traction. Other browsers include Opera, Firefox, Safari and Chrome. Table 4 shows a list of the

---

[12] http://www.securityfocus.com/infocus/1889 for a overview; *Windows Vista and Digital Investigations*, Hargreaves, Chivers, Titheridge, *Digital Investigation*, Volume 5, Issues 1-2, September 2008, Pages 34-48

[13] *A systematic evaluation of disk imaging in EnCase 6.1 and LinEn 6.1*, Byrers and Shahmeri, *Digital Investigation*, Volume 6, Issues 1-2, September 2009, Pages 71-81

release dates of some of the key new versions of some popular browsers. Browser software needs to be updated as the specification for the display and facilities of world wide web pages keeps evolving. As with the table relating to operating systems, there are large numbers of changes within each major version. A very important feature of all browser software is that stores on the user's hard disk copies of the pages visited in what is called a *cache*. The purpose is to speed up the user's browsing experience. As a matter of observation, during web-surfing certain main or index pages on a site will be revisited many times – it makes sense for the user to be able to look at his own cached copy of those pages rather than keep on requesting from the remote web-server. To a computer forensic investigator the cache is invaluable because it makes possible the reconstruction of the user's surfing habits. There are other features of browsers which are forensically useful – facilities for the storage of passwords and to "auto-complete" a web-URL or a user's personal details work because that information is held somewhere associated with the browser – and revealing it may assist an investigation. Specialist software exists to ease this process[14]; however for it to be useful and reliable, such software has to be kept constantly up to date. [15]

Peer-to-Peer file (P2P) sharing services have an even shorter history. This is one of the key the technologies behind high resolution video-streaming facilities such as the BBC IPlayer. It is also used by academia and the computer industry to provide rapid access to large files. But the various versions of P2P have also gained notoriety as they have been used for the sharing of copyrighted material such as music, games and video. They have also been used as a means of distributing pictures of the sexual abuse of children. Depending on how precisely you define the term P2P, the first popular services date only as far back as 1999, when Napster was launched. Significant changes occurred between 2000 and 2002. All of these services require that the user has installed on his PC a "client" program to manage and mediate the sharing. These client programs create records of files searched for, downloaded and shared. These records have been analysed for their forensic value[16]

Even more recent has been the growth of social networking. Facebook, with a claimed world-wide user base of 300 million registered users started with a version for US universities in 2004 and was followed by a High School version in 2005. It has been open to all comers only since September 2006. During that period it has gone through 4 different user interfaces. Facebook claim that 120 million of their users log on at least once a day. LinkedIn, widely used by the business community launched in 2003 but only became significant in 2006; it has about 50 million registered users. And then there is Twitter, which at the time of

---

[14] eg NetAnalysis, http://www.digital-detective.co.uk/netanalysis.asp

[15] There are other features of browsers which may assist the investigator, for example cookies, the small items of text placed there by remote websites during a visit so that, for example, a user can be recognised on a subsequent visit, or to enable such features as "shopping baskets" on a e-commerce site

[16] eg *Peer-toPeer networking issues* Fellows *Digital Investigation* Volume 4 Issue q pp 3-6; *File Marshal: Automatic extraction of peer-to-peer data*, Adelstein and Joyce, *Digital Investigation* Volume 4 Supp 1 pp 43-48 and DRWS 2007

writing is the most popular of the new services with perhaps 18 million users; it was launched in 2006 but its success dates really from early 2009. [17]

Perhaps by now the point has been made; all of these operating systems, applications and services are in very wide use and within all are forensic traces that have significant potential for a very wide range of investigations. The arguments about speed of change in relation to personal computers can be applied with at least equal force to cellphones, where major manufacturers release new models with new features and new opportunities for digital footprints to be created every 3 or 4 months.

Digital Forensics Methodology

Digital Forensic Research Methodologies easily conform to general expectations for scientific work in general and forensic science in particular. Most of the popular operating systems and applications in use today are proprietary and closed source. The product is delivered together with a manual and "help" files to explain the functions and the menuing system, but there is no explanation of how the results are achieved.[18] Few of the products are designed to have forensic qualities, such as full traces of alterations to data, serialing of events and tamper-proofing of log files. The main exceptions are those designed for use in accounting, banking and high security environments.

In order to find in the majority of operating systems and applications material of forensic value, the researcher has to carry out an exercise in reverse engineering, in effect looking at how certain date/time stamps and files are created and changed when particular actions or events take place. The researcher has to carry out many observations, attempt to formulate rules which in effect say: "When this event takes place, the following changes always occur in and to the following files". These rules then have to be tested. Once the rule is known it is possible to write software which will exploit it and turn it into something which an investigator can deploy.

Table 5 shows a typical forensic research methodology.[19]

There is no shortage of outlets for the would-be journal author. The *International Journal of Digital Evidence* is online only but adopts peer review. It first appeared in 2002. *Digital Investigation* is a conventionally published journal published by Elsevier which commenced in February 2004. Others include: *International Journal*

---

[17] It is extremely difficult to keep up with the changes in the Social Networking scene. One semi-reliable place to do so is: http://en.wikipedia.org/wiki/List_of_social_networking_sites

[18] The exception are "open source" products such as the Linux kernel and a variety of Linux-related applications. Here, the products are generated by co-operation and the source code is published.

[19] For a fuller discussion see: *An Examination of Digital Forensic Models*, Reith, Carr Gunsch, *International Journal of Digital Evidence*, 2002 1:3 http://www.utica.edu/academic/institutes/ecii/ijde/articles.cfm?action=article&id=A04A40DC-A6F6-F2C1-98F94F16AF57232D

of Forensic Computer Science (2006); and *Journal of Digital Forensic Practice* (2008).

The first problem is persuading authors to prepare articles to an appropriate level of thoroughness. Much of the discovery of new problems comes from law enforcement investigators. Their priority is always the current case and then the backlog of cases awaiting examination. Few law enforcement employers will allow their officers and civilian employees time to carry out proper research. Although there are now academics specializing in computer forensics, all too often their articles are concerned with technically challenging but seldom-encountered phenomena such as steganography – the techniques of hiding one file within another, or relatively abstract methodological issues. The second problem is the time taken by the peer-review and publication processes. *Digital Investigation* conveniently provides a publication history for each of its articles – when it was first received, any revisions, and when it was accepted. A non-rigorous examination shows that articles seem to take 3-4 months to be accepted and then perhaps to appear 2-3 months thereafter. This is probably relatively rapid when compared with similar processes in academic journals in general. If we add to this period the time taken by the author to research and write-up, even at its best, articles will appear some 12 months after some-one has spotted the forensic potential a piece of software that is wide-spread use.

In practice the main sources of information for the practitioner are relatively informal. There are two main wikis: http://www.forensicswiki.org and http://www.forensicwiki.com/ both run by the "community". There are a large number of websites covering aspects of the topic; some of these are run by enthusiasts for "the community" but others are primarily to sell products and services. The visitor has to decide for himself how much reliance to place on any of these; the quality ranges from the excellent to the dreadful. There are also a number of bulletin boards, some such as *Digital Detective* with a vetting policy for members, others designed to support particular products (and sometimes tied to a maintenance subscription) and some open to all. The main means of quality assurance on a bulletin board is the number of people who are prepared to comment on a problem and its solution. There are also a number of blogs.

A further important source of computer forensics intelligence comes from training schemes. A number of these are largely designed to support particular products; others come from commercial institutes which also offer, for example, training in computer management and security. In the UK *F3*[20] is a well-supported self-help club largely founded by active law enforcement officers where trainers lecture on their experiences for free. Universities also offer courses, from diplomas through undergraduate degrees to masters' and doctoral degrees; however these have to temper the delivery of practical advice with the need for their awards to meet generally accepted academic standards. Most of these schemes do their best but what is not clear is how far all the information imparted has been properly tested.

Testing facilities

[20] http://www.f3.org.uk/

Let's suppose we have some properly peer-reviewed items of technical knowledge of practical value in the investigation of computer hard-disks. We need to turn this into a tool which can be deployed efficiently. Most investigations can be carried out using a very small number of basic utilities; but these utilities require a significant knowledge of operating systems, programming and methods of recording data. Their output may be difficult for the non-skilled to understand. In addition the basic utilities can often only run one query at a time whereas a real investigation often requires high levels of iterative use.

Three informal tests of the quality of a tool are the clarity and transparency of the accompanying documentation, the detail and candour of the change-log, and arrangements for the designer to get customer feedback. The first ought to explain in detail the principles upon which the tool has been designed and what it is supposed to show; the second demonstrates the routes taken by the designers and changes initiated to reach the current version. The third is if the vendor has a bulletin board where customers can post their concerns about anomalies – this is a form of peer-review. Examples can be seen in relation to *NetAnalysis*, a tool for examining the caches of Internet browsers.[21] But none of these approach what is normally meant by full independent testing.

The best established scheme is run by the US National Institute of Standards and Technology (NIST).[22] It says of itself:

> "The testing methodology developed by NIST is functionality driven. The activities of forensic investigations are separated into discrete functions or categories, such as hard disk write protection, disk imaging, string searching, etc. A test methodology is then developed for each category…. After a tool category and at least one tool is selected by the steering committee the development process is as follows: 1 NIST and law enforcement staff develops a requirements, assertions and test cases document (called the tool category specification). 2 The tool category specification is posted to the web for peer review by members of the computer forensics community and for public comment by other interested parties. 3 Relevant comments and feedback are incorporated into the specification. 4 A test environment is designed for the tool category.
>
> "After a category specification has been developed and a tool selected, the test process is as follows: 1 NIST acquires the tool to be tested. 2 NIST reviews the tool documentation. 3 NIST selects relevant test cases depending on features supported by the tool. 4 NIST develops test strategy. 5 NIST executes tests 6 NIST produces test report 7 Steering Committee reviews test report. 8 Vendor reviews test report. 9 NIST posts support software to web. 10 NIJ posts test report to web."

There's little to object to there in terms of methodology and transparency. The problem is that what has actually been tested since the NIST program started in 2002 is only a tiny sub-set of the range of tools that are in actual use and which are

---

[21] Manual incorporated in trial download: http://www.digital-detective.co.uk/downloads.; Change log: http://www.digital-detective.co.uk/changelog/netanalysis.pdf

[22] http://www.cftt.nist.gov/

routinely needed. The fullest tests have been on disk imaging tools and on write blockers (devices to enable a hard-disk to be read while guaranteeing that no contaminating writing to the disk can take place). For "deleted file recovery" and "string search" (running a search across an entire hard disk to look for matches on groups of characters including words) there are simply draft specifications. NIST has decided to value thoroughness over attempting to cover the territory.

Digital Forensic Analysis Suites

The testing methodology we have been discussing is directed at single-function tools, that is, a tool which sets out to exploit a single item of forensically useful knowledge. Such tools were common in the early days of computer forensics and some specialist tools are still popular.[23] But in practice, that's not how most digital forensic investigators operate. For convenience they prefer analysis programs which are in effect integrated suites which offer, among other things, safe forensic imaging of hard-disks, automated recovery of deleted files, a series of viewing environments for the contents of a disk, facilities for examining the contents of a range of complex files, the ability to search across an entire disk, facilities to extract material to produce exhibits, and the automated generation of reports. Typical examples are EnCase [24]and AccessData FTK[25]; there are a number of others. [26]

These tools are popular because they appear to be the only way in which the large number of computers presented for examination can be handled at all. Strong anecdotal evidence suggests that there is a typical 6 to 8 month delay in non-urgent computer examinations in UK police forces. But each of these analysis suites incorporates a very large number of items of "forensically-useful knowledge" and attempts to provide a meaningful way of exploiting all of them. The vendors of these products usually try their best; they employ support staff to deal with queries and complaints, some of them have bulletin boards, most also offer training which brings them into close contact with practitioners.

Table 6 shows, for Encase and AccessData FTK, the frequency with which new versions, updates and bugfixes are released. But none of these are tested in the sense that most forensic scientists and Daubert-like admissibility rules expect. Experienced computer forensics specialists sometime try to address the problem of lack of testing by throwing two competing analysis products at the same task and seeing whether there is any different result. Plainly this sort of approach will identify some

---

[23] eg NetAnalysis (www.digitaldetective.co.uk) ; P2P Marshall (http://p2pmarshal.atc-nycorp.com/); and various collections such as Maresware (http://www.dmares.com/) and the list at: http://www.forensic-computing.ltd.uk/tools.htm and http://www.forensix.org/tools/

[24] http://www.guidancesoftware.com/computer-forensics-ediscovery-software-digital-evidence.htm

[25] http://www.accessdata.com/forensictoolkit.html

[26] For example: X-ways forensics (http://www.x-ways.net/forensics/) ; ProDiscover (http://www.techpathways.com); the open-source Autopsy (http://www.sleuthkit.org/); MacForensicsLab (http://www.macforensicslab.com/)

anomalies which in turn will prompt further inquiry; however this won't work if both products are operating on the same wrong assumptions.

A reconsideration of forensic science within the expert role

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.

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 can involve evaluation and interpretation of ambiguous results[27], reconstruction of events, and the provision of background information about particular commercial practices, technologies and socio-cultural phenomena.

It is 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. The difference can be crystallized around different usages of the word "proof": Scientific proof is the result of a process of investigation, hypthosesis, testing, etc and results in a statement of what is always true (at least until some-one comes and falsifies it). Legal proof is a collection of objects put in front of a court, coupled with testimony as to what has been seen and done and which results in one highly specific conclusion.

It is unfortunate that the Law Commission in its Consultation Paper No 190[28] felt that it was beyond its remit to look at the procedural issues of expert evidence[29] and that the remit of the Forensic Science Regulator is "better forensic science labs."

In fact there is a route within the existing criminal procedure, at least as it exists in England and Wales – it is "Pre-hearing Discussion of Expert Evidence" under CrimPR 33.6.[30]. I have written more extensively about this elsewhere[31] but the Rule can be summarized as follows:

---

[27] See, for example: *Standards for the formulation of evaluative forensic science expert opinion,* Cook, Evett, Jackson, Jones, Lambert, *Science and Justice* 49 (2009) 161–164. See also the remarks of Leveson, LJ, quoted in the *Times*, http://business.timesonline.co.uk/tol/business/law/columnists/article6913109.ece

[28] http://www.lawcom.gov.uk/docs/cp190.pdf

[29] para 1.12

[30] http://www.justice.gov.uk/criminal/procrules_fin/contents/rules/part_33.htm#33.6

- Experts have an over-riding to the court, not their client or employer
- A meeting can either be by mutual agreement or on the order of the court
- The experts generate a document setting out areas of agreement and disagreement in relation to the expert issues, together with supporting reasoning
- Other than that document, the contents of the meeting cannot be referred to without the court's permission
- At a pre-trial hearing a court may make binding rulings about the admissibility of evidence and about questions of law under section 7 of the Criminal Justice Act 1987 sections 31 and 40 of the Criminal Procedure and Investigations Act 1996 and section 45 of the Courts Act 2003

There are several effects:

- One would normally expect experts to agree on matters which are generally scientifically accepted – and for which there is support along the lines of the *Daubert* tests
- Where the area of knowledge is new or tools are relatively untested, opposing experts are committed to find agreement *sufficient for the purposes of the immediate issues before the court* without committing themselves to a more "universal" finding. In order to do so, they may run demonstrations and tests for each others' benefit
- More broadly there are also opportunities for agreed technical explanations, agreed glossaries, and agreed demonstrations for the jury which could simplify and shorten trials where complex technical evidence is significant
- The circumstances of such meetings would need to be settled at pre-trial hearings – PCMHs – and these would have to be appropriately funded
- The Forensic Science Regulator would, as he formulates his regulations for laboratories, need to allow sufficient flexibility for the presentation of evidence which is not fully tested but which an expert is willing to justify for the immediate specific circumstances
- There will be renewed pressure on judges in assessing the expertise of experts. One way forward would be to allow, at a pre-trial hearing, an opposing legal team to mount a challenge, or at least an investigation, of an opposing team's expert
- Judges, in summing up to a jury, may need to consider whether any special warnings about the quality of the evidence should be given.

There is an even more radical procedural approach, which is to allow experts to discuss their differences in front of a court while dispensing with the usual

---

[31] *Meetings between experts: A route to simpler, fairer trials?* Digital Evidence Vol 5, Iss 304, pp 146-152

formalities of examination-in-chief, cross-examination and re-examination. In Australia this is referred to as "hot-tubbing" or more accurately, "concurrent expert evidence"[32] In its current form it is essentially a civil rather than a criminal procedure.

The problem that ICT develops at a rate far faster than related forensic science and tools can be tested will not go away. An inflexible "one size fits all" doctrine of forensic science and the circumstances of its admissibility runs the risk that its consequence will be the walking free from court of many accuseds where digital evidence is significant. A careful adaptation of existing criminal procedures and re-evaluation of the totality of "expert evidence" might provide ways forward.

Table 1: Daubert Tests
Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993) is a decision of the US Supreme Court. Most commentators extract four tests or factors from it; but some also add the fifth one listed here.
1. Empirical testing: the theory or technique must be falsifiable, refutable, and testable.
2. Subjected to peer review and publication.
3. Known or potential error rate and the existence
4. Degree to which the theory and technique is generally accepted by a relevant scientific community.
5. The existence and maintenance of standards and controls concerning its operation.

Table 2: Simplified History of Microsoft Operating Systems		
1984	MSDOS 3	First mature form; character based
1988	MSDOS 4	Able to handle larger chunks of memory

[32] See, for example Cheeseman, Elizabeth in *Bar News: The Journal of the NSW Bar Association* Summer 2006-2007); Edmond*: Merton and the Hot Tub: Scientific Conventions and Expert Evidence In Australian Civil Procedure*, Duke Law School http://www.law.duke.edu/journals/lcp

1990	Windows 3	First mature graphical user interface – but sits on top of MSDOS; later versions in 1992 and 1993 (includes networking)
1991	MSDOS 5-6	Better memory and disk handling
1995	Windows 95	Graphical user interface is whole operating system – not just a program sitting on top of MSDOS
1996	Windows NT4	Version aimed at professional use; improved networking; new system for storing data on disk - NTFS
1998-9	Windows 98 & 98SE	Improvements on Windows 98, better handling of world wide web; USB
2000	Windows 2000	Improvements on NT4
2000	Windows ME	Unsuccessful series of improvements to Windows 98
2001	Windows XP	Until recently the most successful implementation – facilities from both 98 and NT
2006	Windows Vista	Replacement for Windows XP but widely disliked for slowness
2009	Windows 7	Current Version

Table 3: Word processing	
1978	WordStar (CP/M)
1982	WordStar for MSDOS
1982	Wordperfect (MSDOS)
1983	Microsoft Word (MSDOS)

1986	WordPerfect 4.2
1989	Word for Windows
1989	WordPerfect 5.1 (MSDOS)
1993	Microsoft Word 6.0
1997	Microsoft Word 97
2000	Microsoft Word 2000
2002	Microsoft Word XP/2002
2003	Microsoft Word 2003
2007	Microsoft Word 2007

Table 4: Browsers	
August 1995	Microsoft Internet Explorer 1
November 1995	Microsoft Internet Explorer 2
August 1996	Microsoft Internet Explorer 3
September 1997	Microsoft Internet Explorer 4
December 1997	Opera 3
March 1999	Microsoft Internet Explorer 5
June 2000	Opera 4
December 2000	Opera 5
August 2001	Microsoft Internet Explorer 6
Novermber 2001	Opera 6
January 2003	Opera 7
November 2004	Firefox 1
April 2005	Opera 8
June 2006	Opera 9
November 2006	Firefox 1.5
October 2006	Firefox 2
October 2006	Microsoft Internet Explorer 7
June 2008	Firefox 3
September 2008	Chrome public launch
March 2009	Microsoft Internet Explorer 8
July 2009	Firefox 3.5
September 2009	Opera 10

Table 5: Typical Digital Forensic Research Methodology: artefacts on hard disk.
Create “clean” or “virgin” test environment
Make forensic disk image
Introduce changes to be observed
Make further forensic disk image
Look for all the changes
Repeat until you can formulate a rule to describe what is happening
Test rule
Publish
Develop tool
Test tool

Table 6: Updates for Computer Forensic Analysis Suites *Versions and Release Dates*
AccessData FTK
1.60: 30/03/2005; 1.61: 10/03/2006; 1.62: 01/08/2006; 1.70 26/01/2007; 1.70.1 12/04/2007; 1.71: 27/06/2007; 1.72: 18/04/2008; 1.80: 27/06/2008; 1.81: 30/09/2008; 1.81.2: 21/01/2009
EnCase Forensic
3.20: 04/2002; 4.15: 10/2004; 5.05: 07/2006; 6.5.1: 30/05/2007; 6.6: 26/072007; 6.8: 13/11/2007; 6.8.1.: 15/12/2007; 6.10: 06/03/2008; 6.10.2: 06/04/2008; 6.11: 04/06/2008; 6.11.2: 04/07/2008; 6.12: 20/11/2008; 6.12.1: 08/01/2009; 6.13 07/03/2009; 6.14: 14/07/2009