ARTICLE:

DIGITAL FORENSICS SPECIALIST GROUP

By **Miranda Moore QC** and **Simon Iveson**

Miranda Moore QC is a member of the Digital Forensics Specialist Group, and gives her personal impression on the work of the Group and the difficulties in identifying appropriately qualified digital evidence specialists in the UK.

The Digital Forensics Specialist Group (DFSG) was set up in 2007 and held its inaugural meeting in July 2008. It was established to advise the Forensic Science Regulator and the Forensic Science Advisory Council (FCAC). We were given a ten point remit, to support the Regulator and the FSAC by:

1. Identifying requirements for new or improved quality standards applying to the provision of digital forensics services to the police service and the wider criminal justice system. This will include the quality of the techniques employed and of closely associated processes such as evidential integrity, interpretation and presentation of results.
2. Drawing up proposals for such quality standards, following a risk based assessment of priority, for approval by the FCAC.
3. Advising on how to accredit those supplying digital forensics services to the police and to those serving the courts, including the defence, and including in house police services and forensic suppliers to the wider criminal justice system.
4. Advising on how to monitor compliance with digital forensics quality standards.
5. Developing procedures for validating and approving new technologies and applications in the field of digital forensics.
6. Monitoring the availability of training and guidance in digital forensics and making proposals to the FSAC for approaches designed to improve the availability of, and standards in the quality of, training in digital forensics.
7. Advising on measures to ensure the competence of individual practitioners in digital forensics.
8. Creating, tasking, overseeing and managing the output of any working groups required to advise the Specialist group on specific matters within its remit.
9. Monitoring international developments relevant to quality standards in the provision of digital forensics and fostering co-operative links with the relevant international fora.
10. Advising on any other issues concerning quality standards in digital forensics which are referred to the Specialist Group by the Regulator or the FSAC.

The group consists of a diverse cross section of those in the digital field, to some extent I am an outsider because I am an end user, a consumer if you like. I bring to the table the practical, court based problems that an expert will face.

Why is the work of the group so important? From a practitioners point of view it has never ceased to amaze me that one of the most important and everyday items, one used by us all without thinking, causes so many problems when it comes to its analysis as a source of evidential material and its use in court as an evidential tool. The computer is part of our lives, the e-mail, the mobile telephone, the tablet. We cannot function without them. However, they are increasingly used to facilitate a diverse range of criminal behaviour from fraud to blackmail.

With many forensic disciplines it is a straightforward matter to establish the credentials of an expert witness that you may wish to instruct. Pathologists, graphologists, psychiatrists, all have a recognised pattern of training and professional bodies that regulate behaviour and standards. However, there was and still is no one professional body or universal qualification for someone whose expertise lies in the examination and interpretation of digital media.

How does someone in the prosecution or defence camp find an expert? What qualifications should they look for? Are the hours quoted for work and fees reasonable? Will funding be forthcoming to instruct such an expert? Has the expert ever been found professionally wanting? In short am I getting an honourable, experienced, trustworthy, professional witness who uses recognised techniques amenable to review and checking or not?

Staggeringly, when prosecuting I have encountered as the defence 'computer expert' in trials 'the IT bloke from the solicitors firm', 'someone we found on the internet' and 'a guy here doing a favour for a friend'. I have also encountered the use by defence solicitors of certain highly skilled digital examiners whose reports are so long and complicated that the prosecutor takes fright and withdraws the case because it has fallen into the 'too difficult/ too expensive' pile. These reports once analysed often contain very little in the way of actual principled challenge to the Crown's case, however as far as the defence are concerned it was money well spent, because the case collapses.

In the jurisdiction of England & Wales, the defence have a right, generally speaking, to examine the image of their hard drive, seized by the authorities in an investigation. They also have a right, if they can show relevance, to examine other imaged drives in the case. The drives may contain sensitive and personal information. Allied to the issue of security, the legal process needs to be able to check that the person that has been granted rights of examination is competent to carry out the exercise. In one case I prosecuted, the prosecution expert in examining a laptop used for the facilitation of a sexual offence discovered military secrets. He was not security cleared to see what he had found, and I was not sufficiently cleared to know about them, yet I had to persuade a judge to refuse the defence expert of choice access to the hard drive on the basis of his experience and security clearance. If there was a resource where either side in a case could go to find experts, and know their qualifications and experience, the justice system would run more smoothly.

Once defence reports are served, the Crown then has to find an expert to consider and report. This can be a time consuming and expensive process. One would not consider getting a second post mortem report from someone who has watched a couple of episodes of 'Quincy' ('Silent Witness' for my younger readers) or read the entire works of Patricia Cornwell, so why do we take less care with the examination and evidential interpretation of the findings relating to a digital body?

In the early days, our group spent its time trying to understand the scale of the task (problem). In 2010 we took on the responsibility and included within our remit the recovery and interpretation of digital images (such as CCTV). Without a detailed account of the intervening years, where are we now?

I am sure in common with other jurisdictions, when an expert takes the stand, not surprisingly, our courts require them to the give their qualifications, relevant experience and accreditation. Certain words take on different meanings in different professions and disciplines. Accreditation is one which for the courts is akin to an individual's credentials, whereas in laboratory parlance it is about the organisation being accredited to perform a task.

When the group started, it looked to adopting and adapting the ACPO guidance where possible, which touch on skills and competency requirements as well as describing some procedures in some detail. The main output of the DFSG was intended to sit under a larger quality framework; however the consultation on the original framework led to a change of emphasis from a bespoke new standard on forensic science to codes of practice designed to work alongside accreditation. This change in focus towards a 'standard' which would achieve formal accreditation meant it was necessary to think about what the national accreditation body would be looking for. The dynamic nature of digital forensics meant we needed to be descriptive on outcome rather than prescriptive on method. One important feature of accreditation is validation.

There was much debate on the issue of validation, because this takes on different meanings in different professions and disciplines. The traditional 'wet chemistry' forensic science laboratories in the UK have a clear understanding of what validation means in their disciplines and moreover what is required by the national accreditation body. Broadly speaking this is providing objective evidence to confirm that the requirements

Validation is a central policy of accreditation, and more providers, including police laboratories, have shown by attending accreditation that digital forensic methods can be appropriately validated

which define an intended use or application have been met. Specialists in digital forensics appeared to come at it from a software development standpoint and felt it an impossible ask for validation to be a requirement. Software engineers tell me unless they can see all the software code line-by-line then it can never be said to be validated, and even if they did have access, the time consuming nature for a software tool to be used once would be prohibitive. The 'wet chemistry' sciences look to how to test the method with known samples, that is ones that challenge the method without always being as concerned with the internal operation of a commercial. In software parlance, this is 'blackbox' testing which nudges the debate along, although those new to the accreditation requirements will have a learning curve to tailor the amount of testing to be appropriate to the risks to the courts without making the process unworkable. One purpose of the specialist group is to advise and assist the Regulator in forming the debate and identify when to take the debate to the community. Both the Regulator and the group's chair have attended industry specific events to explain why the courts need to know that the method that obtained the information was valid, whether initially it is used as intelligence or was always intended as evidence. Intelligence used as the basis of a dawn raid may well be expected to be used later as evidence, it should be valid even if certain caveats had to be applied. Validation is a central policy of accreditation, and more providers, including police laboratories, have shown by attending accreditation that digital forensic methods can be appropriately validated.

To express this in terms of what will happen at court, validation of methodology will stand as the test for the receipt of evidence, it will reduce the arguments for its admission before the jury, and if experts on both sides are made to meet in advance of the trial (as is now often the case) there will be a reduction of technical discussions before the jury, which often only confuse rather than clarifies the evidence.

The group's work has not been confined to the above, in common with the Regulator's other specialist groups, much of DFSG's business is conducted electronically out-of-committee or by small working sub-groups. For instance, there were a series of sub-group workshops on video analysis from late 2010 into 2011. The February 2012 DFSG meeting was scheduled to coincide with the completion of their endeavours, and this draft video analysis appendix has since undergone technical review with the US based Scientific Working Group on Imaging Technology (SWGIT) and the revised draft and feedback will go to the next DFSG meeting.

The Regulator published a quality framework in December 2011 (after a further three month consultation exercise, extensive revision and several dry runs with forensic science providers) as the Codes of Practice and Conduct (http://www.homeoffice.gov.uk/publications/agencies-public-bodies/fsr/codes-practice-conduct). The various accompanying appendices produced by specialist groups, sub-groups and external commissions will start undergoing consultation in 2012 with the one on digital forensics and video analysis being among the first.
So to conclude, the group's efforts are still a work in progress, we are getting there, but it is only through appropriate industry co-operation and intelligent feedback that we will have a system that will support this 'new' science and bring it in line with the older 'wet sciences' that are so familiar in our courts.

Miranda Moore QC (5, Paper Buildings, Temple, London), has practiced in the area of Hi Tech Crime since 2000 when she began working with the NHCTU. She has been involved in many high profile hacking and computer related cases and has been a member of the Digital Forensics Group since its inception.

Simon Iveson is a member of the Forensic Science Regulator's science team and currently leads the quality standards and digital forensics specialist groups which assist the Regulator in identifying requirements for new or improved quality standards.

