Forensic Science Regulator
Overseeing Quality

Digital Forensics Specialist Group

Minutes of the meeting held on 20th June 2017, at the Home Office, 2 Marsham Street, Westminster, SW1P 4DF

1. Welcome and apologies

1.1 The Chair welcomed all to the meeting. A full list of attendees is available in Annex A.

2. Minutes of the last meeting

21. The minutes of the meeting held on the 18th November 2016 had been approved by members prior to the meeting and were published on GOV.UK.

3. Matters Arising

Action 4: DFSG subgroups to hold first meetings, and report back to a June DFSG meeting.

3.1 The network capture and analysis subgroup had held its first meeting, whilst establishing membership of the open source and cell site subgroups was in progress.

Action 5: Mark Stokes to write to Dave Johnston, to ask whether consideration be given to talking to Communications Service Providers about being able to set up systems and processes for access to test data, so that systems can be tested and validated.

3.2 The Chair had spoken with Dave Johnson. The group heard that Forensic Science Providers (FSPs) would need to access a suitably large amount of test data for validation, and that this data would be anonymised to prevent access to any personal information. Dave Johnson agreed to follow this up with Communications Service Providers.

Action 1: Dave Johnson to follow up with Communications Service Providers on access to test data for cell site validation.

Action 8: DFSG member Jennifer Housego, NPCC open source nominee, to chair a DFSG sub group on open source and social media data.

3.3 This action was in progress, and Dave Johnson agreed to invite Lee Ellis (Metropolitan Police Service - MPS) to be a member of the open source subgroup.

Action 2: Dave Johnson to invite Lee Ellis to be a member of the open source subgroup.

Action 9: Simon Iveson to arrange a police collisions investigation member for DFSG.

Action 10: DFSG to assist with ad hoc digital issues in collisions investigation and refer operational colleagues to the FSR Codes provisions.

3.4 These actions were in progress. The group heard that speed analysis and scene reconstruction, which both formed parts of collision investigations, would need to be accredited by 2020 (provisionally to ISO17020 but potentially to ISO17025). However mobile phones seized in collision cases and digital items designed to be removed from vehicles such as GPS units still came under the Forensic Science Regulator's (The Regulator's) October 2017 deadline for digital forensics accreditation.

Action 3: Simon Iveson to write to the Assistant Chief Constable (ACC) Steve Barry for the nomination of a collisions investigation member for the DFSG if no such member is in place by September.

Action 13: The FSR to forward ad hoc requests from the ISO digital technical committee to DFSG to deal with.

3.5 The group heard that the Netherlands Forensic Institute (NFI) was leading on developing an ISO standard on the interpretation of biometric data. The Regulator advised that this was in it's preliminary stages, but that in the future the UK might seek representation on the group developing the standard.

3.6 All other matters from the previous meeting had been completed or were agenda items for the current meeting.

4. National Police Chiefs' Council (NPCC) Update

4.1 The NPCC representative provided an update on the NPCC's role supporting police forces in achieving the Regulator's October 2017 deadline for digital forensics accreditation to ISO17025. The group heard that mapping was being conducted across 60 legal entities and 6 digital forensics methods. This exercise was being fed through police force quality managers to the performance standards group lead by ACC David Lewis. Once mapping was complete, a highlight report would be produced and made available to the community.

4.2 Members were informed that the NPCC had a portfolio plan to support police forces in gaining accreditation for mobile phone kiosk[1] extractions. The aim was to deliver three tools to allow non-practitioners (e.g. police officers) to perform kiosk extractions. Accreditation for this was hoped to be gained by the end of 2018 through a phased process and the risks of missing the Regulator's 2017 deadline would be

[1] Kiosks: a forensic tool used to preview, triage, copy and extract data. For mobile phones this would include contacts, call logs, and messages.

managed and declared where required. As a part of this process, workshops would be held in October 2017 to support the role out of the technology.

4.3 The NPCC had discussed the definitions of expert evidence and infrequently used methods. The broad requirements for infrequently used methods had recently been discussed at previous meetings of the Forensic Science Advisory Council (FSAC) and the Quality Standards Specialist Group (QSSG). The NPCC would take note of the Regulator's work in this area, and planned to conduct national consultation on what force's considered was included in the infrequency used methods category..

4.4 Police forces reported using different interpretations of the divide between factual and expert evidence, and the NPCC was seeking to provide guidance on this. The group discussed the boundary between factual evidence and expert opinion given by expert witnesses, which was of particular relevance to digital forensics. Police officers and staff were often not operating as (or expected to be considered) experts, but were using the same tools as experts in digital forensics and were required to present findings to the court. This meant that interpretation was often required, and where the finding is open to a different interpretation it could be considered an opinion. Moreover, the use of data fusion tools, where the process leading to an output was poorly understood, and the reporting of this as factual evidence would be complex. The Regulator confirmed that guidance on the contents of expert reports would be issued in due course.

4.5 In collaboration with academia, the NPCC had run a workshop on validation and verification. All material from this workshop would be uploaded to the Police On-line Knowledge Area (POLKA), and a number of forces had uploaded example documents (e.g. standard operating procedures) to this platform.

4.5 The group heard that the College of Policing (CoP) was running a cyber and digital careers pathway initiative. The aim was to create a new qualification to enable individuals to gain accreditation in a range of digital forensic practises. Members indicated that it would be beneficial for the CoP give a presentation on this topic to the DFSG.

Action 4: Simon Iveson to invite CoP to give a presentation to the DFSG on the CoP's planned qualification for digital forensics.

4.6 The representative from the United Kingdom Accreditation Service (UKAS) confirmed that around 70 applications for accreditation in digital forensic practises had been received, with 45 pre-assessments complete. At the time of the meeting nine organisations had gained accreditation, with more expected to do so in the next few weeks.

5. ISO17025 Survey

5.1 The group were informed of a survey apparently conducted on behalf of the First Forensic Forum (F3) on the requirement that digital forensics labs gain accreditation to ISO17025 (general requirements for the competence of testing and calibration laboratories). The survey received 180 responses.

5.2 It was noted that in this survey group there were misunderstandings concerning ISO17025 and how it applied to the field of digital forensics, including those self-declaring a reasonably good or higher understanding. Where there were misconceptions it was clear that it would be beneficial to find the correct forum to correct them. The Chair clarified that ISO17025 should not be regarded as tick-box exercise but as a useful tool to uphold quality standards. The group discussed how the Regulator could engage with stakeholders to improve understanding and debunk incorrect information. It was noted that the Regulator and others had hosted conferences on this topic in the past, but that a question and answer workshop would be a useful way to engage further with stakeholders. It was suggested that the F3 conference might be an option, it was believed that slots may be already oversubscribed. However, F3 does also organise one day workshops, and could look at this option. It was suggested that this workshop should involve a digital forensics practitioner who had successfully gained accreditation, and that the ISO17025 survey was a useful tool for indentifying topics to be discussed during the event.

Action 5: Danny Faith to scope out options for running a Q&A workshop on gaining accreditation for digital forensics with F3.

Action 6: John Beckwith to help identify digital forensics practitioners to speak at the Regulator's workshop at the F3 event.

5.3 The group note that there were likely to be other conferences related to digital forensics where delegates would benefit from representation by the Regulator.

Action 7: Tim Watson to provide the Regulator with a list of relevant conferences related to digital forensics.

5.4 Members heard that the BCS Chartered Institute for IT and the Institution of Engineering and Technology (IET) provide software validation tools and background material for teaching courses. The group agreed it would be useful to engage with the BCS and IET in order to explore the possibility of including digital forensics in these courses.

Action 8: The Regulator and Tim Watson to discuss approaching the BCS and IET with a view to including digital forensics as a component of their teaching courses.

5.5 It was also suggested that the Regulator may wish to engage with stakeholders concerning accreditation through short online video clips. It was proposed that these had the potential to reach a greater audience than traditional methods of stakeholder engagement. In addition, Gloucestershire Constabulary was

already involved in a similar activity and would be happy to assist the Regulator on this matter if required.

Action 9: The Regulator and Jennifer Housego to discuss the potential of engaging with stakeholders through online video content.

6. Reliability of mobile phone extractions

6.1 The group was presented with a document from UKAS, outlining the extraction of data from mobile phones and the reliability of these extractions. The document posed a number of questions to the group concerning the type of outputs produced, the tools used and the validation required.

6.2 Members heard that different tools were producing different results from the same input data, and that as a result customers were being provided multiple outputs. It was highlighted that different organisations were likely to be using different tools, and that the police needed to have confidence in the result they produced. This issue was underpinned by limited test data available for some handsets. It was suggested that it would be beneficial for a repository to be set up where quality test data could be uploaded to compare different tools. The group was asked to consider the questions posed by the UKAS document and provide feedback electronically.

Action 10: DFSG members to provide David Compton with feedback on the reliability of mobile phone extractions within two weeks.

7. Accreditation requirements for mobile phone kiosks

7.1 The group was presented with a second document from UKAS outlining the accreditation requirements for mobile phone kiosks. Kiosks could be deployed at multiple sites, outside of traditional hi-tech crime areas, such as at crime scenes. As such, this presented unique challenges for accreditation. The group was invited to discuss how accreditation for kiosks might be implemented.

7.2 Members discussed that kiosk deployments at multiple locations presented a challenge, and that test environment data should be collected to help validate tools that move between locations. It was emphasised that this would be a significant issue for multiple areas of forensic science in the future, as forensic tools become increasingly mobile. In addition, the group discussed how ISO17025 could be applied at sites of kiosk deployment.

7.3 It was suggested that there were three potential options for kiosk deployment accreditation: fixed sites (e.g. a specific kiosk in a specific location), known sites (e.g. a police station) and unknown sites (e.g. a crime scene). The group heard that the Metropolitan Police Service (MPS) was seeking accreditation under option two.

7.4 It was agreed that the group would produce additional guidance on this matter via email directly to UKAS.

Action 11: DFSG members to provide advice via email to David Compton concerning the accreditation for mobile phone kiosks within two weeks.

8. Mobile phone kiosk validation

8.1 Members were given an update on validation of mobile phone kiosks by the Centre of Applied Science and Technology (CAST). The group was presented with a diagrammatic overview of the mobile phone examinations by kiosks, which detailed the various stages of the process. It was cautioned that methodologies between police forces varied, and the diagrams produced by CAST were aimed at establishing a standard process.

8.2 The group heard that there was no single standard covering mobile phone examinations by kiosks, and were presented with a document outlining the criteria required for validation of this technique. Two of the key requirements were completeness and reliability of the data extracted. Key to interpreting the output of kiosks was an understanding of the limitations of different tools. UKAS had already provided feedback to CAST on the validation requirements, and the next step would be to develop tests for these requirements.

8.3 The group discussed corrupted and incomplete data, and it was suggested that such data could be included as part of the validation test data. It was highlighted that experts within digital forensic laboratories should be consulted on where the risks with this technology laid. It was confirmed that a risk assessment of the process was required, as was stress testing of the tools.

8.4 It was enquired how this process would be completed in a coherent and inclusive manner. It was suggested that centralisation and standardisation would save police forces time.

8.5 The amount and type of data required for validation was discussed, including how to achieve representative samples from very large data sets. Consideration was also given on how to establish and maintain these ground truth data sets. It was suggested that as many handsets as possible should be included. The group heard that the police had consulted on the most prevalent handsets involved in investigations, aiding CAST in identifying the range of handsets required for validation.

8.6 Members highlighted additional considerations such as the risk of double counting data, a preference amongst practitioners for a rage of tools, a lack of central governance and the need for blind trials.

8.7 CAST agreed to share the documents presented to the DFSG with the group via email for further consideration, particularly in relation to the type of data that should be included for validation of mobile phone kiosks.

Action 12: Neil Cohen to email DFSG members copies of the mobile phone kiosk validation documents presented at the meeting.

9. Cell Site Update

9.1 The group received an update on a pilot run by UKAS on cell site analysis[2]. Despite a good uptake by providers originally, there had been a substantial drop-out rate. As such the pilot consisted of two complete assessments for radio frequency RF propagation surveying[3] and no assessments of site analysis were carried out. Issues were encountered with a lack of ground truth data with which to validate the tools. Members also heard that the pilot highlighted variation between organisations conducting this work.

9.2 UKAS would continue the pilot and address some of the issues encountered, in order to be able to provide a recommendation on accreditations timescales for cell site surveying to the Regulator.

10. AOB & Date of the Next Meeting

10.1 No items of any other business were raised.

10.2 The next meeting of the DFSG would be on the 22nd September 2017 in the Home Office.

[2] Cell site analysis includes the acquisition of communications data and the processing of those data, often in association with data captured during a radio frequency (RF) propagation survey.

[3] A radio frequency survey is undertaken to determine what mobile phone masts are able to provide service at a location or in an area or along a route.

Annex A

Present

Mark Bishop	Crown Prosecution Service (Brighton)
John Beckwith	Staffordshire Police (via teleconference)
Neil Cohen	Centre for Applied Science and Technology, HO
David Compton	United Kingdom Accreditation Service
Danny Faith	First Forensic Forum (F3) Steering Committee
Jennifer Housego	NPCC Open Source Nominee
David Johnston	Gloucestershire Police
Mark Stokes	Metropolitan Police (Chair)
Matthew Tart	CCL Group Digital Forensics
Gill Tully	Forensic Science Regulator
Tim Watson	Warwick Cyber Security Centre

In attendance

Simon Iveson	Forensic Science Regulation Unit, HO
Thomas Vincent	HO Science Secretariat