Forensic Science Regulator
Overseeing Quality

Digital Forensics Specialist Group (DFSG)

Note of the meeting held on 7 November 2019, at the Home Office, 2 Marsham Street, Westminster, SW1P 4DF.

1. Welcome and introductions

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

2. Minutes and actions of the previous meeting

2.1 The minutes of the meeting held on the 13th June 2019 had been approved by members prior to the meeting and would be published on gov.uk.

2.2 The following matters arising from the previous DFSG meeting were discussed:

a. Action 1: NPCC representative to liaise with the Regulator and FSRU on a representative who could join the DFSG Open Source sub-group. It was confirmed that the existing NPCC representative would remain on the group.
b. Action 2: Staffordshire Police representative to update the DFSG on the outcome of their pre-assessment with UKAS at the next meeting. This action would be discussed under agenda item 2.
c. Action 3: Staffordshire Police representative to circulate the forensic findings document to members of the DFSG. This action was in progress and the document would be circulated to the DFSG members following the meeting.
d. Action 4: The Regulator to circulate first draft of the Digital Forensics paper to DFSG members for comment in July. Comments had been received from DFSG members and would be discussed under agenda item 7.
e. Action 5: The FSRU to form a sub-group for the investigation of digital forensics at scenes. A sub-group had been formed, and an update would be provided to members under agenda item 3.

f. Action 7: The First Forensic Forum representative to send the FSRU their comments on the definition of digital forensics. This action was complete.
g. Action 8: The Staffordshire Police representative to send the FSRU their comments on the definition of digital forensics. This action was ongoing, and the Staffordshire Police representative would share their comments with the FSRU.
h. Action 10: The NPCC representative, FSRU, and the Regulator to arrange a meeting to discuss the standard scope for Open Source intelligence/Internet Intelligence and Investigations. The Regulator met with the NPCC representative, and options on standards were being considered. A draft appendix had been prepared and circulated for comments. The NPCC representative confirmed they were undertaking a peer review for open source network to identify best practice, and this would be used to produce guidance.

3. Frontline kiosks

3.1 The Staffordshire Police representative provided the DFSG with an update on their pre-assessment with UKAS.

3.2 The NPCC had published a national level one kiosk validation package in April 2018. The document specifically looked at the level one method for logical acquisition of data from mobile devices. This piece of work had been developed in partnership with Dstl. The package included user guides, standard operating procedures, and validation results and focused on the three main kiosk providers in the market at the time. The aim was to validate once to avoid repeated validation at different local entities who wish to use this package, therefore, it was important to ensure the validation package was up to date. Staffordshire Police had submitted a proposal to Transforming Forensics (TF) to update the validation package where required. A small working group was working on this within Staffordshire Police.

3.3 It was confirmed Staffordshire Police had applied for an extension to scope for the accreditation of the methods used. The pre-assessment was held on the 18th of July 2019. Staffordshire Police received positive feedback on their validation, and the pre-assessment highlighted an issue they were already aware of concerning verification against user requirement. The pre-assessment

identified more work was required around the issue of verification against user requirement. Some options would need to be sought to address this issue to ensure this method would be accreditable to ISO 17025. After the pre-assessment Staffordshire Police reviewed these findings and had further discussions with Dstl on possible options available.

3.4 Staffordshire Police met with UKAS and the Regulator to discuss how to progress with the validation accreditation and identify other options and resolutions available. This would ensure they could develop a national validation package for policing. A verification options paper was being developed, and once complete this would be shared with UKAS and the Regulator for their comments. The verification options paper would look at two specific aspects, the scope and verification. The scope had been defined as very limited in data acquisition. The verification would be examined in two parts which were, what could be done in the short term to ensure verification against user requirement was accreditable, and in the long term how to improve the tooling used and engagement with suppliers.

3.5 The Regulator provided the members with her views on this issue. There had been early discussions on what the requirements should be for kiosk type deployments. There had been an increase of the use of tools by front line officers as there had been an increase in mobile devices being seized. There was an issue with the range of outputs from the kiosk depending on the device being integrated. The Regulator commented on a need to ensure that kiosk users, generally non-experts, were able to identify when the kiosk had not returned the expected information. The members discussed whether the limitations of the kiosks outweighed the usefulness however, the representative from Staffordshire Police highlighted that only 10% of level one cases proceeded to level two so the level one kiosk was providing useful information.

3.6 The Regulator would recommend that each legal entity include one kiosk method on their scope of accreditation. Frequent software updates had highlighted the need for a national validation approach, and users would need to be aware of additional functionality that came with software updates. The representative from UKAS stated that they were looking at what level of change

to software would require a verification and reassessment. The UKAS representative recommended the Staffordshire Police approach for validating software.

4. Investigation digital forensics at scene

4.1 After reviewing the wording in the Codes it was decided a longer definition of digital forensics at scenes was required. A small working group was formed with representatives from National Crime Agency (NCA), and Digital Media Investigators (DMI). The working group were tasked with identifying the risks associated with performing digital forensics activities at scenes. The working group identified that there were challenges when performing digital forensic activities at scene, as there was a risk of losing data from the device. It was important to identify what the digital forensic crime scene equivalents were for the digital forensic lab-based techniques.

4.2 A member suggested inviting the South East Regional Organised Crime Unit (SEROCU) to the sub working group. The SEROCU could offer useful guidance on on-scene acquisition. The DFSG members were asked if they would also like to join the sub group. Representatives from UKAS, Dstl, and F3 volunteered to join the sub group.

Action 1:

4.3 Staffordshire Police representative to share SEROCU contact information with the FSRU.

Action 2:

4.4 UKAS, Dstl, and F3 representatives to join the sub-group.

4.5 The Regulator queried what the outcome of the working group would be. The working group would develop a definition of digital forensics at scenes and identify the areas that were accreditable and the areas that were not accreditable. The group would also focus on risk assessments on the types of digital forensic activities performed at the scene. The group would identify possible risks that could be controlled for example by accreditation or centralised standard operating procedures.

5. Definition of digital forensics

5.1 The members discussed the draft text for a definitions appendix for digital forensics which had been circulated to members prior to the meeting. A larger document would be produced in 2020 which would define all the terminology for forensic science. The members were also presented with the emerging text for the Statement of Standards and Accreditation Requirements in the Codes. This text included all activities that required accreditation. The members were asked if the two documents included all of the required information. It was confirmed that the Statement of Standards would be published within the next few weeks.

5.2 The UKAS representative confirmed they were undertaking a project on reviewing their definitions for digital forensics as they had observed variation at different organisations. The term “extraction” had caused confusion, UKAS defined extraction as extraction of data from data while some users define this as extraction of data from a device. The new terminology for the different stages included capture, preservation, processing (converting it into a human readable format) and analysis. The Staffordshire police representative was supportive of this project and felt this would support the police forces with their accreditation.

5.3 A member queried whether reconstruction of data files should be included within the digital forensics definition. For example, if fragments of data were used to reconstruct the original data file. It was argued this would not be correctly described as process or analysis and separate category was suggested, such as “reconstruction” or “restoration”.

Action 3:

5.4 Members to send more information on the reconstruction process, and further comments on the Statement of Standards to the FSRU within the next week.

5.5 On the definitions document a member suggested highlighting the cloud element in terms of the examination of a relevant device to locate, extract or recover any information on the device.

5.6 A member queried the inclusion of forensic collision investigation in the exclusions list of the definitions document and whether this would fall within the definition of digital forensics. It was confirmed that forensic collision

investigation would be covered under a separate forensic collision investigation standard.

6. Indecent images of children and the Child Abuse Image Database (CAID)

6.1 The Regulator presented this item. The Regulator had received a number of referrals concerning indecent images of children, specifically around inappropriately graded images, or images that had not been graded at all. The Regulator sought views from the DFSG if these referrals would come under the remit of the forensic science Regulator (FSR) as part of digital forensics and if not, then who should these referrals be raised with.

6.2 The members agreed grading indecent images of children was not within the remit of digital forensics. A member suggested referrals for indecent images of children should be raised with the NPCC portfolio lead for Child protection and abuse.

6.3 The Regulator also raised the issue concerning the Child Abuse Image Database (CAID) and if this was within the remit of the FSR in terms of oversight and developing standards for national intelligence databases. Members were asked if the regulator should be setting standards for CAID.

6.4 The members agreed this was a national intelligence database. Automated classification of images on this database was discussed and members agreed that this would fall under the remit of digital forensics. Members suggested it would useful to have a discussion with CAID to discuss this topic further.

Action 4:

6.5 The FSR and the FSRU to liaise with the CAID team to discuss whether automated analysis of child abuse images would be in the scope of the Regulator.

7. Digital Investigation paper

7.1 The Regulator provided the DFSG with an update on the Digital Forensics paper for the *Digital Investigation* journal. The paper would need to be

completed and submitted by next week. The Regulator had received comments from some members of the DFSG and was in the process of collating them. The Regulator would be sending a final draft version to the members who had provided comments as soon as possible.

7.2 The members were asked to provide final comments on the paper and confirm if they were happy to be listed as authors and to provide their information directly to the Regulator as soon as possible. The Regulator thanked the members for their comments and contributions.

8. Data retention and back up

8.1 The UKAS representative presented this item. The issue of data retention and back up and how this was interpreted within the codes, had been raised by the UKAS technical assessors. The UKAS representative sought advice from the DFSG on this issue. The UKAS understanding of data retention was that all data generated should be backed up and stored at a separate location. This often involved imaging of hard disks and storage media that often included large amounts of data.

8.2 The purpose of data back up by FSPs was discussed and the Regulator advised that this was to prevent loss of original data whilst held at the FSP. The group discussed who should retain data. When a police force had commissioned an FSP to carry out the work the FSP would not be expected to retain the data, it would be the responsibility of the police force to retain and back up the data. The members discussed issues with returning data in that FSPs were unable to collate different cases on the same storage hard drive resulting in a wastage of space on storage devices, additionally data was not always returned to the accredited part of the force.

8.3 A member highlighted that one purpose of the backup was to create a copy of the data that could be read in the future as it was not always possible to rely on the original IT to access the data, for this reason some practitioners outside of policing would retain data indefinitely. This raised a retention issue.

8.4 A working group had been created to review data retention guidance in police forces. Another member mentioned the Investigatory Power Commissioner Office was also conducting research on storage of data.

Action 5:

8.5 Gloucestershire Police representative to find out more information on the Investigatory Power Commissioner Office research on storage data.

8.6 A member highlighted the need for clarity in terms of data retention, and how long data should be held for. A member queried who was responsible for the data retention policy. It was confirmed the Home Office was responsible for the data retention policy. The Regulator explained the Codes aimed to ensure organisations were working to the same standard.

Action 6:

8.7 Home Office representative to meet with CPS representative to discuss the data retention policy for digital forensics.

8.8 The representative from the Warwick Cyber Security Centre also queried when the backup would be required to be created, an immediate backup may increase the risk of a ransomware attack as it would require the use of an always-on network.

8.9 The Regulator informed the group that an interim position would be agreed with UKAS at a meeting in the next week. This discussion would look at standards requirements but would not consider customer requirements.

9. Validation

9.1 The validation sub group meeting would be held after the main DFSG meeting. The main areas of focus for the working group would be assessment of risk and errors within the method validation in Digital Forensics document.

9.2 The Regulator emphasised clearer guidance would benefit the digital forensic community.

9.3 The representative from F3 asked about guidance on creating test data, the representative from the FSRU responded that this depended on user requirements.

Action 7:

9.4 Representative from FSRU to liaise with representative from F3 on user requirements for test data.

10. AOB

10.1 The date of the next meeting as confirmed as Wednesday 17 June 2020.

Annex A

Organisation Representatives Present:

Home Office (co-chair)

United Kingdom Accreditation Service

Gloucestershire Police

NPCC Collision Investigation Nominee

Forensic Science Regulator

Metropolitan Police

F3 - The First Forensic Forum

Staffordshire Police

Dstl

NPCC

Warwick Cyber Security Centre

CCL Group Digital Forensics

Crown Prosecution Service

Forensic Science Regulation Unit, HO

HO Science Secretariat