



Digital Forensics Specialist Group

Minutes of the meeting held on 13th June 2019, at the Home Office, 2 Marsham Street, Westminster, SW1P 4DF

1. Welcome and apologies

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

2. Minutes and actions of the last meeting

2.1 The minutes of the meeting held on the 13th December 2018 was agreed by members and had been published on GOV.UK.

2.2 Action 2: FSRU to collaborate with MPS representative to produce an article ahead of next meeting. This action would be discussed in agenda item 4.

2.3 Action 4: Dstl and NPCC DCG representatives to liaise regarding guidance for open source. The DFSG Open Source sub-group had been established to advise the Regulator on quality standards for open source forensic investigations (Internet Intelligence and Investigations). There had been a change of representatives in the group and this had delayed the progress.

Action 1: NPCC representative to liaise with the Regulator and FSRU on a representative who could join the DFSG Open Source sub-group.

2.4 Action 5: The Regulator to meet NPCC representative and discuss whether third party applications should be out of scope from the level 1 service and how this should be reported in the validation declaration. This action was now complete. An accreditation pilot for frontline kiosks would run in January 2019 with third party applications out of scope. This was due to the findings of UKAS, who in reviewing the Dstl validation study observed limitations on the extent of data obtainable from third party applications and opined that this would not be an accreditable activity. It was confirmed Staffordshire Police had submitted an application for accreditation. The pre-assessment with UKAS would be held in July 2019.

Action 2: Staffordshire Police representative to update the DFSG on the outcome of their pre-assessment with UKAS at the next meeting.

2.5 Action 10: Gloucestershire Police representative to provide an update on the third-party standard at the next DFSG meeting. This was still currently in progress and would be deferred until the next DFSG meeting.

2.6 All other actions were complete or would be covered under later agenda items.

3. Error Investigation

3.1 There had been an increase of referrals to the Regulator concerning digital forensics. Due to the number of different referrals for digital forensics, it was decided more lesson learnt documents should be produced; five lessons learnt documents had been produced to date, and several were directly concerning digital forensics.

3.2 The types issues raised to the Regulator concerning digital forensics, included inaccuracies, misinterpretation, evidence handling which included loss of data, overwriting of data, and sending data to the wrong individuals or organisations.

3.3 Issues had also been raised on the tools used when analysing digital forensics. An example was given where a software tool used had produced results that were later shown to be incorrect. Further investigation by the software provider revealed an error in the software that was subsequently fixed. It was agreed by the DFSG the software providers should do more to investigate and resolve the errors as soon as possible, and also update all FSP's that use their software.

3.4 Another example of issues with the tools used in digital forensics was mentioned. During the validation testing of a tool it was discovered it was reporting deleted data as live data. It was emphasised that the validation testing requirements must include a number of risk assessments conducted during different stages of the validation process. It was important the methods used for validating the risks was considered the best methods available. Two documents had been produced that provided validation guidance. The documents were called digital validation, and general validation. Both documents required updating, and it was suggested including more information around the methods used to conduct risk assessments within these documents. The DFSG were asked if it would be useful to include this information or was there enough information already in the documents. The Staffordshire Police representative mentioned they had been developing guidance on 'forensic findings'. The document included what methods had been utilised for digital forensics and the risks of these methods.

Action 3: Staffordshire Police representative to circulate the forensic findings document to members of the DFSG.

4. Outline of magazine article

4.1 The Regulator had been contacted by the editor of Digital Investigation to produce an article on digital forensics. The Regulator was keen to produce an article based on actual data rather than opinion. The Regulator presented the DFSG with a paper on the proposed structure for the article. The Digital Investigation magazine was producing a special issue on digital forensics, and the deadline for submissions was 30 August 2019. The Regulator was keen to produce a paper and submit it before the deadline. The DFSG were asked if there was anything else that should be included in the proposed paper. The DFSG were happy with the content in the proposed paper and had no further information to add.

Action 4: The Regulator to circulate first draft of the paper to DFSG members for comment in July.

5. Digital incident scene forensics

5.1 The DFSG had previously suggested that a sub-group should be formed to assess application of standards for incident scene investigation/management in the 'digital age'. Members were asked if a sub group should be formed, and what its scope should be, or should it be merged with the network sub group. The DFSG favoured forming a sub-group for incident scene investigation, and this would be a separate group to the network sub group. It was suggested members should include representatives from policing, and FSP's.

Action 5: The FSRU to form a sub-group for the investigation digital forensics at scene.

6 Definition of digital forensics

6.1 The Codes of Practice and Conduct contains a short definition of digital forensics; a requirement had been identified to give great clarity about what areas are subject to the provisions of the Codes. The DFSG were asked for suggestions on what should be included within the definition of digital forensics, and the codes definition of digital forensics. A member highlighted it was important that the scope should be sufficiently broad and covers all the items that had been discussed within the group. It was suggested broadening the term "from the device" to include "or accessible from the device", and this would include the cloud, and the internet. The First Forensic Forum representative confirmed they were also in the process of updating their definition of digital forensics and was happy to share this with the FSRU.

Action 6: The UKAS representative to send the FSRU their comments on the definition of digital forensics.

Action 7: The First Forensic Forum representative to send the FSRU their comments on the definition of digital forensics.

Action 8: The Staffordshire Police representative to send the FSRU their comments on the definition of digital forensics.

6.2 A member raised a concern on areas within digital forensics that were considered outside the scope of accreditation for example, new emerging tools or technologies. The UKAS representative explained that in time the use of a flexible scope could resolve this issue, but this would only be possible once the level of quality standards was mature enough.

Action 9: DFSG Members to send written feedback to the FSRU on the definition before the 21 June 2019.

Action 10: NPCC representative, FSRU, and The Regulator to arrange a meeting to discuss the standard scope for Open Source intelligence/Internet Intelligence and Investigations.

7. Commissioning ground truth datasets

7.1 The Regulator recognised there was a difficulty in the digital forensic community to keep up with the standards. The Regulator was keen to make the process easier for the digital forensics community. The Regulator proposed developing datasets that would be accessible to everyone within the digital forensic community. This could assist in the community in keeping up to date with testing and validation. The DFSG were asked if they could define what was required for the datasets or would this need to be commissioned by someone else on behalf of the DFSG before a request was submitted to the commissioning hub. Members were supportive of the proposal.

8. Cell site pilot

8.1 A pilot of cell site validation for accreditation had commenced a year and a half previous but had been paused due to various issues. The FSRU had written out to the digital forensic community recently informing them that pilot would recommence. Expressions of interest from six digital forensic providers had been received. The timelines for commencing the pilot had been received from the interested providers and were for dates next year.

8.2 Improvements in practice were required and the DFSG were asked to consider the issue and advise the Regulator accordingly.

9. AOB

9.1 A member provided a brief update on forensic collision investigation. It was predicted vehicle forensics telematics may be of interest in the future.

10. Date of next meeting

10.1 The next meeting would be held on Thursday 07 November in Westminster.

Annex A

Present

Home Office (co-chair)
Forensic Science Regulator
Staffordshire Police
CCL Group Digital Forensics
F3 - The First Forensic Forum
Dstl
United Kingdom Accreditation Service
NPCC Open Source Nominee
Forensic Science Regulation Unit
HO Science Secretariat

Apologies

College of Policing
Metropolitan Police
Crown Prosecution Service (Brighton)
University of Canterbury
Cyber Security Centre - University of Warwick/ CSFS
Warwick Cyber Security Centre
Metropolitan Police (co-chair)
Gloucestershire Police
NPCC Collision Investigation Nominee
Warwick Cyber Security Centre
CCL Group Digital Forensics