Forensic Science Regulator
Overseeing Quality

Digital Forensics Specialist Group (DFSG)

Note of the meeting held on 3 November 2020, via teleconference.

1. Welcome and introductions

1.1 The Chair welcomed the members to the meeting. A full list of the attendee organisations and apologies is provided at Annex A.

2. Minutes and actions from the last meeting

2.1 The minutes had been circulated to members and would be published on the FSR website.

Action 1:

2.2 Secretariat to publish November 2019 minutes.

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

a. Actions 1 and 2: these actions related to digital forensics activity at a scene and the scene activity working group had held their first meeting. There actions were complete.

b. Action 3: A statement of standards was issued with the Codes of Practice. This action was complete.

c. Action 4: This action required definition of the aspects of CAID that would fall under the remit of the regulator and this action was ongoing.

d. Actions 5 and 6: These actions related to data retention and this would be discussed further at this meeting. These actions were ongoing.

e. Action 7: Discussions with F3 on user requirements for test data had been held and this action was complete.

3. Extraction of data from a complainant’s mobile phone

3.1 A representative from Digivault provided with the DFSG with a presentation on a proposal that a NPCC group was considering which involved crypto-hashing data from a complainant’s mobile phone at the point of acquisition and only allowing access to the data with the owner’s express permission, and biometric.

3.2 The main points of the presentation were:

a. Digivault develop systems for secure storage for digital assets and they had developed a block chain solution to share commercially sensitive data in a searchable encrypted format.

b. A Digivault solution could be designed to capture data from a complainant’s phone in an encrypted format. This would allow police to collect the data “blind” and the complainant could decide whether to give consent for the police to access that data at a later time.

c. Hashing algorithms could be used to “time stamp” the recovery of the data.

d. The data recovered could only be decrypted with the complainant’s consent using a biometric key that was linked to them. A layered encryption solution would be used so that certain key props, such as mobile phone numbers or dates and times, would be encrypted but would become searchable.

e. It would be possible for a request to be made to search for a specific piece of data, for example a text message between two known numbers on a specific date. If that data was present on the device a specific request could be made to the complainant for decryption for a specific purpose.

f. Holding the data in an encrypted format would provide confidence to the CPS and defence that data was held by police, and confidence to the complainant that the data cannot be accessed unless for a clear purpose.

g. Every time data was accessed or queried an auditable data trail would be created using block chain. The purpose of the block chain was only to act as a time record that could not be amended.

3.3 The members made comments on the presentation:

a. The representative from the Warwick Cyber Security Centre suggested that the creation of an auditable data trail could be achieved using a simpler method such as a Git repository, this was agreed by the Digivault representative.

b. The representatives from Dstl and Transforming Forensics (TF) observed that recovery of a complete set of data from a mobile device was notoriously challenging and if the data was recovered "blind" it may be difficult to confirm that all the data had been recovered. The representative from TF also noted that it would also be difficult to search or analyse the encrypted data if it hadn't been packaged in the appropriate way for forensic analysis.

3.4 The representative from Digvault clarified that the aim of technique being developed was directed more towards a complainant's phone, rather than a suspect's phone, where analysis of data may focus on specific queries rather than full analysis. Further discussion of the tool was welcomed to overcome the challenges.

3.5 The representative from the FSRU observed that in terms of standards a tool of this type could be considered in the same way as the digital kiosks. Manual verification was important for kiosks and therefore the representative was concerned that this approach would lack of manual verification. There was also a concern that if a conviction was secured the complainant could withdraw permission to access the data and this may affect the appeal process.

3.6 The representative from TF was noted that the tool presented was a mechanism for encryption and it was not clear whether it would address the gap in legislation highlighted by the ICO.

3.7 It was agreed that further discussion with groups such as the DFSG would be required to take the development of the tool forward and members were asked to send their questions and comments on the tool to the representative from Gloucestershire Police.

Action 2:

3.8 Members to send any questions or comments on the Digivault presentation to the representative from Gloucestershire Police.

4. Law commission report on search warrants

4.1 The Home Office had asked the Law Commission to conduct a review of the law governing search warrants and produce proposals for reform.

4.2 The Law Commission had published its report and made 64 recommendations.

4.3 The report included four chapters on electronic evidence, including acquisition of cloud data.

4.4 The member representing the First Forensic Forum (F3) had provided members with a summary of the report and the DFSG were invited to consider the report, identify matters which fall within the remit of the Regulator and advise on any quality standards and remedies that might be required.

4.5 The Regulator was interested in the position of the Home Office in terms of the policy response to the report.

4.6 The Chair would liaise with the relevant Home Office Policy team to provide the DFSG with an update on the Policy position.

Action 3:

4.7 Home Office Policy Team to feedback on policy issues in recovery of cloud-based data

4.8 The UKAS representative highlighted there were challenges with quality control regarding the deletion of data or return of devices as there was no recourse to return to the data to investigate any problems identified later. The representative from the University of Warwick noted that digital forensics required integration of a large amount of data to answer specific questions and therefore retention of complete data sets, rather than a representative proportion, wold be required if the evidence needed to be returned to.

4.9 The representative from Dstl highlighted that in terms of cloud data it would be possible that the jurisdiction that the data was held in may be unknown.

Therefore, any guidance provided should be broad and not specific to a particular jurisdiction.

4.10 The representative from Dstl also noted that there was a cross-over with the discussion of recovery of data from a mobile phone in that some of the data that could be recovered from a phone may be held on a cloud but accessed through the phone. The representative from F3 agreed with this and commented that policies, processes and legislation should reflect that data would increasingly be held in a variety of cloud-based locations.

5. User requirements

5.1 The Regulator explained that validation requirements in the Regulator’s Codes of Practice state that procedures need to be validated against the defined user requirement. This defines what the testing the should cover and what the limits of the deployment should be. If the user requirements were not well understood this would present challenges in producing ground truth databases (GTD).

5.2 The representative from F3 highlighted a need to provide assistance to digital forensics groups with defining their end-user requirements and sought good practice examples from the DFSG.

5.3 The Regulator noted that Microsoft had offered to run workshops to assist with identifying good practice examples.

5.4 The representative from Dstl observed that one of the biggest challenges in the validation of mobile phone kiosks was defining the user requirements and agreed that there was need for better guidance in this area.

5.5 The representative from the FSRU noted that CAST had previously produced a document on user requirements or system processes and suggested that this could be updated.

Action 4:

5.6 FSRU representative to locate the CAST document on user requirements for validation.

5.7 The representative from the Forensic Collision Investigator Network highlighted the need for specific regional end user requirements when a national approach was taken.

5.8 The Regulator sought examples of where user requirements have been well defined and suggested that the FCN could be approached to assist with that.

Action 5:

5.9 FCN to provide DFSG with examples of well-defined end user requirements

6. Ground truth datasets for digital forensics

6.1 The Regulator had asked Dstl to investigate data sets that could be produced to help labs with accreditation and so in validation of digital forensics.

6.2 Dstl had sent out a spreadsheet to relevant stakeholders, including forces, and commercial labs, asking what techniques they were looking at and which ones were a priority. A summary of the findings had been produced which took out areas where practitioners said they already had a data sets and then scored on frequency of use and need for the data set.

6.3 Using this approach phone-based data sets was identified as a main priority. Although laboratories may have accreditation for phone analysis it was flagged that maintaining an up to date phone-based data set was a problem because it was a rapidly evolving area.

6.4 The representative from Dstl noted a challenge with regularly updating data sets for phone-based data was the need for multiple phones and was looking into solutions where data could be provided without the need for a set of physical phones.

6.5 Another priority for a data set was in making sense of large amounts of data, such as file carving.

6.6 It was noted by the Dstl representative that the data collected was a snapshot and may not be fully representative and was seeking advice from the DFSG on research priorities.

6.7 The group was in agreement with the research priorities identified.

6.8 The Regulator highlighted that TF had identified child exploitation was a priority for them so this would beneficial for Dstl to include.

6.9 The representative from Dstl concluded that the first priority would be phones and the second would be advanced data processing, which would also help with child exploitation investigations. Dstl will liaise with TF and FCN as to what is automation was needed for this.

Action 6:

6.10 Dstl to seek the views from TF and FCN on their priorities for data sets for accreditation and validation processes.

7. Learning standards for digital forensics/cybercrime and Digital Media Investigators

7.1 The Regulator introduced this item which had arisen from attendance at the NPCC performance and standards group where a request was made for feedback on digital forensics learning standards. The Regulator noted that there was no reference to FSR standards in the College of Policing (CoP) learning standards for digital forensics and thought this was a good opportunity to have something included in these standards. The DFSG was asked for views on the most important areas to include.

7.2 The representative from CCL Forensics noted that one of these learning standards was aimed at future experts but there was no discussion of forensic issues or standards. There was a risk about inference from the methodology suggested by the CoP and the CoP may need guidance on this.

7.3 The Regulator suggested that changes to these learning standards should be brought to the DFSG for comment.

7.4 The representative from UKAS agreed that the standards should have reference to quality procedures, particularly following procedures and what to do if it was necessary to go against a procedure. It would be advantageous for the standards to give an overview of what quality standards should be in place to increase awareness and understanding of the requirements, such as the headings from ISO 17020.

7.5 The representative from the NPCC (Digital Trust and Evidence) would expect to see these headings and should be in a position to influence this from policing side.

7.6 The Dstl representative also raised the issue of testing of tools and asked for the learning standards to include reference to how to test tools before they are used.

Action 7:

7.7 The Regulator to collate comments and feedback to the College of Policing on their learning standards and offer specialist input from the DFSG

8. DFSG Sub group updates

8.1.1 The representative from the FSRU gave an update on the work of the DFSG sub groups. It was noted that progress had been affected by the Covid-19 pandemic and cancellation of conferences and meetings.

8.1.2 The cell site group had been set up to produce an appendix document to assist with cell site analysis which was complete and future work would focus on the pilot. Results from the pilot would be expected in the coming 6-12 months.

8.1.3 On digital scene examination sub group meetings had been held and crossover had been identified with network forensics. Both the scene examination and network forensics groups would restart once FSRU staff had full access to MS Teams. These groups may need to be merged or renamed as a result of the crossovers.

8.1.4 The representative from the NPCC (Internet Intelligence and Investigations) updated the group on the Internet Intelligence and Investigations (III) capability which had completed production of an internet investigations training module. A pilot was being run to ensure there were no gaps however the module was available for forces to use. An additional training module on covert investigations was in development. The Triple I conference had been moved to a virtual event and had over 1000 delegates registered. The representative informed the group that a new III capability manager would be appointed in due course and an interim point of contact would be in place in the meantime.

9. AOB

9.1.1 The Regulator informed the group that she would remain in post for three months to the middle of February to allow for a smooth transition to the new Regulator.

9.1.2 The representative from the cell site sub-group asked if the DFSG could provide an update at the next meeting about inference in digital forensics and academic work in this area, this was noted by the Chair.

9.1.3 The next meeting would be in around 3 months, date to be confirmed.

Annex A

Organisation Representatives Present:

Home Office (Chair)

Forensic Science Regulator

CCL Forensics (for the cell site sub-group)

Criminal Prosecution Service (CPS)

Cyber Security Centre

Dstl

First Forensic Forum (F3)

Forensics Capability Network (FCN)

Forensic Collision Investigator Network (FCIN)

Forensic Science Regulatory Unit (FSRU)

Home Office (secretariat)

National Police Chief's Council (NPCC) - Digital Trust and Evidence Group

National Police Chief's Council (NPCC) - Internet Intelligence and Investigations

UKAS

University of Warwick

Apologies: