Forensic Science Regulator
Overseeing Quality

DIGITAL FORENSICS SPECIALIST GROUP

Minutes of the 18th meeting, held at 11:00am on Friday 18 November 2016 at the Home Office, London

1.0: Welcome and Introductions

1.1 The Chair welcomed all present to the eighteenth meeting of the newly reformulated Digital Forensics Specialist Group (DFSG). See Annex A for the full list of attendees and apologies. The Chair hoped that the absent members could participate in the future meetings

2.0: Introduction from the FSR: Gill Tully

2.1 The Forensic Science Regulator (FSR), Gill Tully, explained that she was a DNA scientist with a firm understanding of the rules of evidence but limited digital knowledge, so would rely on DFSG to support her with expertise across the range of digital forensics disciplines. Thus the group would need to include the police portfolios for digital forensics, and academics with digital expertise. Thanks were expressed to Tim Watson from the Cyber Security Centre for joining DFSG. New digital technologies had recently developed, in particular relating to communications, networks, social media and open source data. Appropriate digital forensics accreditation standards were needed, hence the recent reformulation of DFSG membership.

2.2 The group aimed to set proportionate digital forensics standards, and to ensure provision of reliable digital evidence for the courts. DFSG would also act as a reference group for future digital forensics issues, and if the FSR gained statutory powers, then it would gain a wider role advising on the related standards.

3.0: Outline of DFSG aims by Chair: Mark Stokes

3.1 The DFSG chair, Mark Stokes, outlined the role and work of DFSG, explaining that it would encompass all types of digital evidence, as technological progress led to digital forensics spreading into new areas. In particular the development of the Internet of Things (IoT) would result in many new types of digital devices interacting with each other. A button-sized wearable computer with communications capabilities had already been developed, for example. All types of digital evidence provided to courts needed to include uncertainty estimates.

3.2 There was an issue of a transition, from collection of digital data by police officers with a range of competencies, to provision of expert witness digital evidence in court, which thus needed to meet expert witness evidence standards. Witnesses who did not consider themselves expert might give opinions in court, perhaps when pressurised by barristers. Thus, suitable controls needed applying to the court statements. There were parallel examples from disclaimers stated by other police witnesses in court. Also education around the issue could be provided for judges.

3.3 The main aims for the current DFSG meeting were to define the DFSG working groups needed, the members required for them and the timescales for their work.

4.0: UKAS update on digital accreditation

4.1 The United Kingdom Accreditation Service (UKAS) representative explained that the pilot exercise on Cell Site Analysis (CSA) was needed, as this was a new area for accreditation, and would ensure that UKAS could apply the standards consistently.

4.2 UKAS had issued expressions of interest for the CSA pilot late in 2015, and seven organisations had joined it. UKAS accreditation pre-assessments for CSA were held in June 2016, at which point six organisations remained. Applications for accreditation were invited, and five of the organisations applied. Inter-laboratory comparison was needed, with proficiency testing, so a controlled known scenario was set up against which to test.

4.3 It was accepted that the data captures and/or surveys completed by the organisations across a range of days could be affected by various factors, including changes in the weather. An organisation might suffer a low score because weather conditions affected their survey. That said, the reality was that there would be time elapsed in historical Radio Frequency (RF) surveys, and any variations might also indicate the robustness of the method.

4.4 The assessment visits had been planned for September to December 2016, but given delays with organisations complying with procedures and validating methods, would be from January to March 2017. The four remaining organisations might in fact all have the assessments carried out by David Compton and a UKAS technical assessor in March 2017.

5.0: Future Digital Forensics Specialist Group Work-streams

5.1 The proposed DFSG sub groups needed to be of appropriate size. Large groups could become “talking shops” and small ones could lack a range of experts for all the diverse areas. Neil Cohen would arrange appropriate subject matter experts from Home Office (HO) Centre for Applied Science and Technology (CAST) for the proposed sub groups.

5.2 The sub groups would need guidance from DFSG on their role, in order to define the support they needed. Membership could potentially include

police officers, engineers, lawyers, and more generally both technical and subject experts. The sub group chairs would invite additional members with relevant expertise.

5.3 Sub group members would typically need six weeks notice for meetings, so the first meetings would be in late January or early February 2017, either at Home Office Headquarters or at Forensic Science Regulation Unit (FSRU) offices in Birmingham. The sub groups would first report back at a DFSG meeting in June 2017, providing papers two weeks in advance, or verbal reports, assuming that DFSG met quarterly. Simon Iveson would support the sub groups.

Action 1: Simon Iveson to discuss with the DFSG sub groups the support they need.

Action 2: DFSG sub groups to send membership lists to DFSG for review, and DFSG sub group chairs to invite further members for the range of digital disciplines.

Action 3: Neil Cohen to arrange HO CAST members for the sub groups.

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

6.0: Cell Site Analysis and Communications Data Sub Group

6.1 CSA was an area needing further standards work as well as widening to cover all communications data, thus requiring a specific DFSG sub group on the forensic issues.

6.2 However, there were ongoing concerns with the quality of CSA forensic evidence, for example the use of the phrase “consistent with” in statements, for example “This data is **consistent with** the suspect being at the given address”, without being clear it was consistent with them being in many other places also. The published appendix made clear that the use of the phrase **consistent with** was not considered good practice in statements.[1]

6.3 DFSG discussed the scope and membership for the CSA sub group. Wifi surveys were touched upon in the CSA appendix, but more detail might be required, so expertise in this area was sought. 3G, 4G, 5G and 6G mobile networks would need covering, so input on the potential new technologies was also required, and it was suggested that “RF and Electro-Magnetic (EM) mapping and geo-location” could be a comprehensive title for the sub group, as it required mapping of these emanations, followed by geo-location using this map.

[1] For example in R v. Puaca [2005] EWCA Crim. 300121, Lord Justice Hooper commented that: “Whereas ‘inconsistency’ is often probative, the fact of consistency is quite often of no probative value at all.”

6.5 Sets of test data (from test calls, not real customers' data) from Communications Service Providers were needed for use in testing and validation of CSA and Communications Data forensic processes by third parties. The Communications Capabilities Development Programme could assist.

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.

7.0: Network Data Capture and Analysis Sub Group

7.1 DFSG reviewed the work needed on digital forensics for network data capture and analysis, as they would need to reach a view on the appropriate standards, which had been flagged as forthcoming in the FSR Codes. Networks primarily involved data encapsulated in "packets", and analysis of a digital network from an end-point. In considering the digital processes required for this kind of forensic evidence, and colleagues with the relevant expertise, digital networks penetration testers were appropriate. The Cyber Security Centre had colleagues with three levels of expertise in this area.

7.2 Within digital networks analysis, router analysis could be included under International Standards Organisation (ISO) 17025 laboratory accreditation, while the in situ networks would be accredited against the ISO 17020 standard for crime scenes. DFSG needed to consider both traditional data networks comprising cables plugged into wall-sockets, and newer "Zigbee" networks, with wireless low-power radios providing personal networking. Data needed capture from a live system, with a simultaneous incident response. The network under investigation could be supporting a business and thus need to continue operation during the investigation.

7.3 For this work, a DFSG sub group would be set up on network capture and analysis. The Pareto principle (or 80/20 rule) would be applied, because of the diversity of these technologies, to achieve an emphasis in the standards on the more important types of networks.

Action 6: A DFSG network capture and analysis sub group to be set up, to propose technologies to be included under digital networks, and submit the proposals to DFSG.

Action 7: Tim Watson to arrange for a colleague from his Cyber Security Centre to chair the DFSG Networks sub group, which would have members from the City of London Police, Financial Service Authority, Serious Fraud Office, and the Competition and Markets Authority.

8.0: Capture and Analysis of Social Media and Open Source Data: DFSG Sub Group

8.1 DFSG considered the issues for validation and accreditation of forensics for social media and open source data. An open source conference, attended by the FSR a month previously, had sought to professionalise the subject, attempting to assess the risks in data capture and interpretation in this difficult area. The area was growing, as police officers routinely searched for data on laptop computers, collected it, and interpreted it at court. The Office for Security and Counter-Terrorism was re-writing the codes defining when a Directed Surveillance Authorisation permit was needed for digital investigations such as these.

8.2 Parts of these procedures might not qualify as forensic science, and which aspects needed accreditation to ISO 17025 standards was to be decided. Validation procedures and competence testing would also be required. For accreditation, searches across the internet for these types of data might be speculative searches instead of tests. The searches could be assessed by repetition by several individual forensic specialists, with comparison of the results.

8.3 Individuals were writing digital tools to collect data from the internet without necessarily having relevant expertise. For example there were five or six online tools of uncertain quality available on the internet to track an individual's activities. These used the subject's mobile phones and their geo-tags on internet posts, on the "Facebook" site for example. Issues included how these tools performed, and with whom they shared the data, typically advertisers. The tools were used by police officers to recover data for evidence, but procedures varied, and on occasions poor quality screen-prints were used to record the information. Tools stated to be free for personal use probably required payment for police operation.

8.4 To simplify evidence, the chain of evidence for court statements could be considered to start from the time of retrieval of the data from the internet, instead of from the time it was posted up. The Crown Prosecution Service would explain how Open Source data should be presented in court

8.5 DFSG member Jennifer Housego, the NPCC open source lead, was recommended as chair for the DFSG sub group on open source and social media data, with support from DFSG. CoP had also been contacted seeking an open source DFSG member.

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

9.0: Collisions Investigation Data

9.1 Work was under way in a separate group on the forensics processes in road vehicle collision investigations. The types of data collected in these investigations to include under the FSR's digital accreditation deadline of October 2017 needing clarifying. Collisions Investigators worked in particular with Closed Circuit Television images, and Global Positioning Systems (GPS), carrying out vehicle speed estimation. They calculated the required uncertainties of measurement for some types of data. The scope for a DFSG sub group on this topic could be recovery, analysis and interpretation of digital forensic data from vehicles.

9.2 Digital equipment capable of removal from a vehicle was sent to a digital forensics laboratory for analysis after a road traffic incident. However, GPS might require analysis in situ. Data was also downloaded from digital devices installed into vehicles by insurance companies. Further data was obtained from motor manufacturers such as Bayerische Motoren Werke (BMW), having been streamed from the vehicle to them, and obtaining this data took more time.

9.3 Many types of vehicles could be considered for this digital forensics analysis, for example, cars, buses, trams, lorries, trains, boats or even aerial drones, but all contained computers with common properties of storing volatile and non-volatile data, and suffering data changes when forensically examined. Hence the same issues arose across digital investigations for all vehicles types

9.4 DFSG would need to answer questions on digital forensics for operational colleagues. For example, HO CAST had been asked about a potential test device to establish whether a driver was texting at the time of a road traffic accident, for future routine use in collision investigations, similarly to routine breathalyser testing. Therefore DFSG needed a Collisions Investigator as a member, and they had been approached but not yet replied. Apart from this ad hoc support to colleagues, DFSG would not generally work further on specific collision investigation forensics, with the possible exception of speed estimation. Digital forensics colleagues would be referred to the existing guidance and standards in the FSR Codes.

Action 9: Simon Iveson to arrange for 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.

10.0: AOB

Digital requests from the international digital technical committee

10.1 The FSR chaired the British Standards Institute (BSI) Forensic Science Processes (FSM/1) committee and received requests on digital forensics issues from the ISO / TC 272 mirror technical committee on digital forensics. DFSG agreed to deal with these issues when they arose. All relevant international standards covering digital forensics would be reviewed, but only considered for adoption in United Kingdom if they were suitable for accreditation and the FSR agreed.

Action 11: The FSR to forward ad hoc requests from the ISO digital technical committee to DFSG to deal with.

UKAS issues with validation of police "digital kiosk" tools

10.2 UKAS had encountered issues with the various deployments encountered with "digital kiosks" for front line officers, as some were mini-hi-tech crime laboratories instead of simple kiosk deployments. In particular UKAS needed to see an effective method for assessment of the uncertainty of measurement of these tools. Dual-tool validation and testing also needed attention. David Compton would draft a paper on these issues for DFSG.

Action 12: David Compton of UKAS to circulate a paper outlining the issues with UKAS accreditation of digital kiosk technology to DFSG.

Annex A

Present

Mark Stokes	Metropolitan Police (Chair)
John Beckwith	Staffordshire Police
Mark Bishop	Crown Prosecution Service (Brighton)
Neil Cohen	Centre for Applied Science and Technology, HO
David Compton	United Kingdom Accreditation Service
James Luck	Metropolitan Police
Gill Tully	Forensic Science Regulator
Tim Watson	Cyber Security Centre

In attendance

Simon Iveson	Forensic Science Regulation Unit, HO
Mike Taylor	HO Science (Secretary)

Apologies

Danny Faith	First Forensic Forum (F3) Steering Committee
Jennifer Housego	National Police Chiefs' Council, Open Source Lead
David Johnston	Gloucestershire Police
Nigel Jones	Canterbury Christ Church University
Matthew Tart	CCL Group Digital Forensics