

Report from a Digital Evidence “fitness for purpose” workshop

Present at the workshop on 15th December 2009

- Mr. A. Marshall (n-gate ltd. & Forensic Science Society, Workshop organiser)
- Mr. A. Rennsion (Forensic Science Regulator)
- Dr. T. Watson (De Montfort University, facilitator)
- Eur. Ing. B.C. Tompsett (University of Hull, facilitator)
- Mr. L. Allen (SOCA)
- Mr. R. Kelly (Data Duplication Ltd.)
- Mr. S. Janes (Computer Forensic Alliance)
- Mr. D. Lucas (HMRC)
- Mr. T. Wise (Forensic Mobile Services)
- Mr. R. Russell (Forensic Telecommunication Services)
- Dr. R. Baxter (Metropolitan Police)

Apologies received from : Mr. C. Carmichael-Jones (LGC Forensics), Mr. R. Patel (Afentis Forensics), Mr. K. Cottenden (CY4OR), Dr. B.A. Price (Open University), Mr. M. Dickinson (Systemation AB), Mr. M. Larson (CCL Forensics)

Purpose

1. The draft digital evidence appendix to the Quality Standards for Forensic Science Providers document includes a principle which states that the provider “..shall have the ability to demonstrate that any tools, techniques and methods are fit for purpose.” The workshop was instigated to allow Forensic Science Providers (FSPs), Forensic Tool Providers (FTP) and End Users (EUs) to discuss the meaning of this principle and suggest ways in which it can be complied with.
2. The intention is not to produce a draft standard or method for compliance but to explore possible ways forward and, if possible, to produce a roadmap or framework for further work leading to an accepted and acceptable mechanisms which can be adopted by FSPs, FTPs and EUs.

General discussion

3. There was some general discussion of the proposed standard and a common theme was that it might be considered unnecessary or inappropriate to focus on tools. It seemed to be generally accepted that processes, which are implemented by tools, are the critical elements which might need to be subjected to scrutiny of some sort. Furthermore, there is currently no requirement for accreditation of expert witnesses, thus it could be argued that accreditation of processes is inappropriate as processes must be carried out by people who are qualified to perform them.
4. It was also suggested that, as originally captured data is always available, tests can be repeated independently to confirm or refute findings and that, as such, it could be sufficient to rely on the current situation where the accused has the right to instruct their own expert.
5. It was also considered important that any “fitness for purpose” regime should include mechanisms to deal with processes and tools developed in-house, provided as open-source or adapted from “non-forensic” sources (ad-hoc).

Purpose

6. Before tackling the large challenge of identifying mechanisms to demonstrate fitness for purpose, the issue of “purpose”, in the context of digital evidence, was discussed.
7. During discussions it became clear that the concept of “purpose” is variable and somewhat nebulous as it seems to depend on the nature of the investigation being conducted and the stage of the digital process.

8. For example, it may not always be necessary or possible to have a complete copy of all data from a storage device (e.g. where the device is damaged or during capture from a live system where data are changing during collection). The purpose of a capture tool could, in this situation, be stated as “recovering as much data as is possible reliably” from the device.
9. The difference between recovery for evidential purposes vs. intelligence purposes was also briefly mentioned. Discrepancies might be more tolerated in intelligence gathering tools than in those used to produce material to be used directly in court.
10. It was generally agreed that definitions of “purpose” could not be reduced to one or two simple phrases and that it would probably be more appropriate to define a set of requirements (in the software engineering sense) for digital forensics, dependent on the phase of the process, the nature of the devices and the nature of the enquiry.
11. By selecting these requirements early on in the enquiry appropriate tools could be identified. It was also suggested that correctly defined requirements could be used to assist in the formulation of forensic strategy.
12. For “standard” cases or tasks, pro-forma sets of requirements might be produced and used as a basic benchmark for tools. Non-standard cases/tasks would require the production of unique sets of requirements which may not be satisfied by extant processes or tools.
13. Based on conventional software engineering principles, once requirements are properly identified and confirmed it becomes possible to define tests for validation and verification using white box and black box methods, including tests for abnormal or exceptional operation.
14. Future requirements could be identified well in advance (e.g. for issues such as forensic examination of “cloud” data or virtual environments) and used to inform process and tool development.

Demonstration of fitness for purpose

15. Once a set of requirement has been identified, as noted above, it becomes possible to prepare test cases and data. These can be used to show fitness for purpose as purpose is defined by the requirements.
16. Discussion next turned to the issue of who should take responsibility for demonstrating fitness for purpose. Although the draft standard suggests that this is, ultimately, the responsibility of the FSP there are several ways it could be achieved
 - i. FSP internal. As part of their accreditation, FSPs could establish themselves as test laboratories and perform the testing in-house. This allows them to deal with commercial and in-house processes and tools, as well as open-source and ad-hoc, but may prove costly for smaller providers or those who develop a significant number of new techniques. Costs and efforts will be duplicated as each provider will be carrying out similar testing.
 - ii. FTP internal. FTPs could become accredited as test labs. and, as with FSP testing, carry out testing themselves. Again, this may be costly and may pose a further problem where a requirement is established that competitor's products must co-exist on the same workstation as commercial confidentiality may prevent full testing in this situation. FTPs are also unlikely to be able to test all possible configurations of equipment in use by client FSPs. Testing of in-house, open-source and ad-hoc methods may not be possible in this model.
 - iii. FTP external. Using a service such as CESG's Claims Tested Mark, an independent service allows FTPs to have their tools tested by an independent third party. However, the cost of such testing is not insignificant and it may also introduce delays into product lifecycle because of the time taken. This option may also struggle to cope with the equipment configuration issue

mentioned above and is unlikely to be able to deal with the in-house, open-source or ad-hoc categories.

- iv. FSP external. An independent testing body could be established on behalf of the FSP industry. As an accredited test laboratory it would operate to the same standards as others. Its remit and operational model could require it to test any tools and/or processes at the behest of its customers. Costs would be distributed and duplication of effort could be reduced to a minimum. As an industry controlled body, this test lab. would be required to ensure that tests were carried out on the major configurations and could deal with the co-existent tools problem which is difficult to address in options ii) and iii) above.
 - v. Register of issues. Rather than testing tools and processes they should be assumed to be fit for purpose unless shown otherwise. A register of issues could be established, controlled by an independent body, such as F3 or the FSP external agency (option iv), through which errors and discrepancies can be reported and confirmed.
 - vi. Leave as is. In the current situation, the courts are used to establish what is and is not acceptable. It was suggested that there may be no good reason to change the existing system which allows for independent scrutiny of the evidence prior to and during the trial process.
17. If some sort of testing is to be performed, it is clear that different types of tools & processes will require different types of testing. Data collection is, perhaps, the most crucial as all other phases currently depend on it. Other phases may not be testable in the same way as it may be difficult to establish “correctness” of interpretation of imaged data.
18. Calculation of error rates for digital forensic systems is difficult as there are no reference databases and few verified test data sets available.

Recommendations

19. Work should be supported to establish sets of requirements for “standard” cases, ideally leading to development of requirements for “future crimes”.
20. Work should be supported to establish a National Digital Evidence Database and/or sets of standardised test data which can be used for testing and the possible establishment of error rates.
21. As the above points and recommendations seem to lead to the possibility of a prototype framework for digital evidence process & tool testing, a pilot project dealing with forensic data collection (including, but not limited to, imaging) should be established to explore the framework further. It may be appropriate for this project to include the Digital Evidence Database and Register of Known Issues.