

Workshop on “Fitness for Purpose” of digital forensic tools

Background

The current Forensic Science Regulator's draft standard for digital evidence contains a principle that forensic science providers “shall have the ability to demonstrate that any tools, techniques and methods” are fit for purpose.

This implies a strong need for accepted/approved validation/verification procedures for all stages of the processes involved in processing digital evidence in any form whatsoever. While some of these are implicitly shown to be fit for purpose through their application in other forensic disciplines (e.g. measures to establish continuity, antic-contamination procedures etc.) the majority of software and hardware based data capture, recovery and examination tools are unique to the digital evidence “industry”.

Whereas other forensic sciences use methods which are well established in other, related, scientific disciplines (e.g. medicine, pharmaceuticals etc.) and based on established, published, scientific principles, the systems used in digital evidence work are more reliant on reverse engineering methods to interrogate filesystems and other storage systems which are subject to revision at short notice and at the whim of the manufacturer.

Commercial confidentiality tends to prevent the providers of the tools from disclosing their test procedures, data and logs.

Furthermore, the tools used in digital evidence work run, on the whole, on general purpose computers which are of different specifications. Although subject to a minimum specification there has been no work done to demonstrate that one particular combination of hardware and software produces identical results to another when examining the same evidence source. Thus, the issue of configuration management may be considered relevant in some situations. In fact, this is similar to the requirement to re-accredit in other disciplines following changes in equipment configuration or adoption of new technology.

Therefore, it is entirely possible that every service provider seeking accreditation under ISO17025 or equivalents may find themselves in a situation where they are required to carry out significant levels of basic testing on each and every configuration which they use in order to satisfy the validation/verification requirements. Not only this, but in the event that new hardware or software is deployed tests may have to be repeated before the results from these new tools can be used.

Aim

The aim of this 1-day workshop is twofold :

- firstly to establish if the validation/verification problem is that identified above
- secondly to propose means by which the industry can satisfy the validation/verification requirement without increasing costs and replicating work unnecessarily

Participants

Participants will be drawn from the 3 major sectors identified : tool providers (hardware & software), service providers (forensic scientists) and service users (law enforcement and legal representatives) in order that all views can be represented and considered appropriately. Participants should not be members of the existing digital evidence group to ensure that views are completely fresh and independent.

Schedule

09:30-10:00 Coffee and registration

10:00-10:15 Welcome (A. Rennison)

10:15-10:45 Discussion points from the standard & existing research (A. Marshall)

10:45-12:00 Breakout 1 – discussion of validation/verification (coffee available)

12:00-13:00 Lunch

13:00-14:00 – Reports from Breakout 1 – identification of key issues/themes

14:00-15:30 – Breakout 2 – solutions to issues identified in Breakout 1 (coffee available)

15:30-16:00 – Reports from Breakout 2

16:00-16:30 – summary of Breakout 1 & Breakout 2 – topics for the proposal document

Breakout groups will be no more than 3 or 4 people representing each sector identified and all discussions will be under Chatham House Rules.

Outcome

Following the conclusion of the meeting, a draft report/proposal will be circulated to all participants for comments/amendments. The final document will be submitted to the Forensic Science Regulator for wider dissemination and consideration.