

This is a repository copy of *Requirements in digital forensics method definition : Observations from a UK study*.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/137032/>

Version: Accepted Version

Article:

Marshall, Angus M. and Paige, Richard orcid.org/0000-0002-1978-9852 (2018) Requirements in digital forensics method definition : Observations from a UK study. Digital Investigation. ISSN 1742-2876

<https://doi.org/10.1016/j.diin.2018.09.004>

Reuse

This article is distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs (CC BY-NC-ND) licence. This licence only allows you to download this work and share it with others as long as you credit the authors, but you can't change the article in any way or use it commercially. More information and the full terms of the licence here: <https://creativecommons.org/licenses/>

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

Requirements in digital forensics method definition: observations from a UK study

Angus M. Marshall, Richard Paige

Dept. of Computer Science, University of York, UK

Abstract

During a project to examine the potential usefulness of evidence of tool verification as part of method validation for ISO 17025 accreditation, the authors have examined requirements statements in several digital forensic method descriptions and tools. They have identified that there is an absence of clear requirements statements in the methods and a reluctance or inability to disclose requirements on the part of tool producers. This leads to a break in evidence of correctness for both tools and methods, resulting in incomplete validation. They compare the digital forensics situation with other ISO 17025 accredited organisations, both forensic and non-forensic, and propose a means to close the gap and improve validation. They also review existing projects which may assist with their proposed solution.

Keywords: ISO 17025, ISO 27041, quality standards, method validation, Tool verification, forensic tool development

1. Introduction

ISO/IEC 27041 [1], as part of a group of standards dealing with digital investigations, is the standard which describes a process by which a method can be shown to be fit for its intended purpose. To achieve this, it proposes a process for the validation of methods used in a digital investigation. Within the description of validation it suggests that evidence of a tool's verification against a declared set of requirements can be used as means to reduce the amount of validation required for processes in which the tool participates.

Email address: `angus.marshall@york.ac.uk` (Angus M. Marshall)

This work was supported by the University of York Research Priming Fund

9 i.e. it suggests that those process requirements which are wholly satisfied by
10 the tool, and for which evidence of verification exists, need not be subjected
11 to further testing.

12 Note: in this project we have concentrated solely on the validation and
13 verification issue. The other standards in the group propose models of evi-
14 dence gathering and processing which. although useful, are not considered
15 core issues for this work.

16 From the perspective of software engineering the proposal in ISO/IEC
17 27041 [1] is entirely acceptable. However, for such a mechanism to succeed,
18 the tool and the process in which it participates must be specified in terms
19 of requirements which can be mapped against each other to show how the
20 tool conforms to, or partially fulfills, the requirements of the process.

21 In effect, the proposal is that there is some degree of overlap between tool
22 requirements and method requirements, ranging from the possibility that a
23 tool's requirements are a complete subset of a method's requirements (Figure
24 1) to the, potentially, less likely situation where a method's requirements are
25 a subset of a tool's (Figure 1).

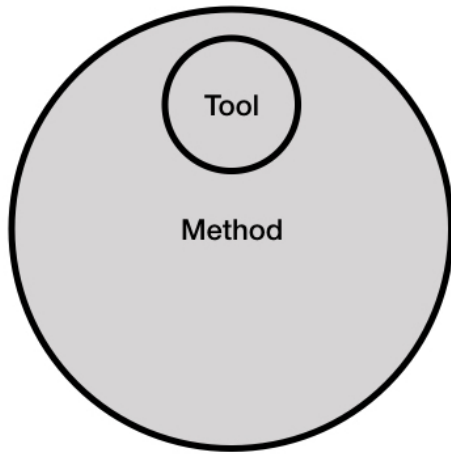


Figure 1: Tool requirements are a subset of method. Typical of specialist tools or small tools produced to assist with part of a method.(Shaded area = the set of requirements which must be satisfied for validation.)

26 In practice, because some of the requirements for a method with an inves-
27 tigative context will be non-technical in nature, it is believed that the most
28 common situation will be that shown in Figure 1, where a tool's requirements

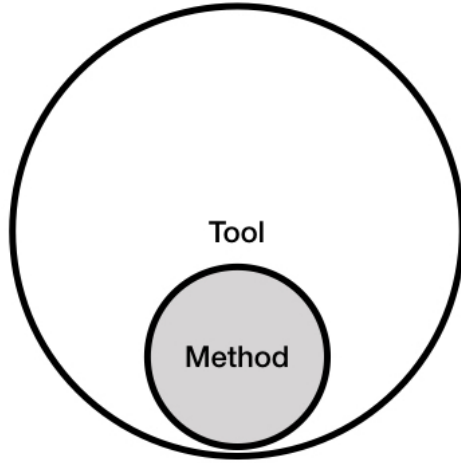


Figure 2: Method requirements are a subset of tool. Considered rare, but possible where a method exactly follows a process defined by the tool producer and uses only a subset of the tool functionality. (Shaded area = the set of requirements which must be satisfied for validation.)

intersect with those of a method, and only those tool requirements lying in the intersection are relevant to the validation of the method.

During research into how this mechanism could be applied in practice, particularly to allow producers of tools for digital forensic processes to support their customers' compliance with ISO 17025's² validation requirement [2], through disclosure of evidence of testing and without compromising commercially sensitive information such as details of test data, the authors have found that such a mapping appears, at the time of writing, to be impossible to perform. This is because it has proved impossible to obtain the necessary levels of information about requirements from any of the participants in the study. Two main factors appear to affect this:

- Firstly, the process definitions examined in our study do not contain any technical requirements which can be mapped. Rather, they contain primarily non-technical requirements aligned to the needs of the

²In this document we concentrate on the use of ISO 17025:2005 as the currently deployed standard. We consider the implications of transition/update to the 2017 version in the Conclusions of this document

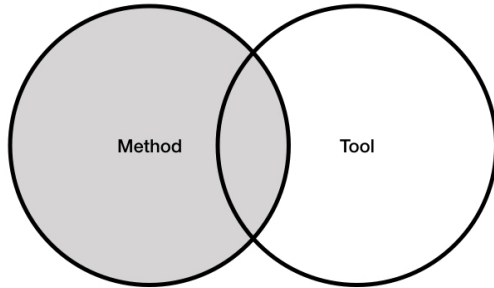


Figure 3: Tool requirements intersect with the method. Common where the tool fulfils some or all of the technical requirements, but there are other non-technical requirements to be satisfied. (Shaded area = the set of requirements which must be satisfied for validation.)

Criminal Justice System.

- Secondly, the tool producers are either unable (in the case of most small providers) or unwilling (in the case of most larger providers) to provide information about how they capture customer requirements, let alone disclose what those requirements are.

Some even went as far as responding to the request for information with statements such as “The information you seek is commercially sensitive as we operate in a very competitive landscape. Unfortunately, we can’t give out any specifics on our product development techniques to third parties.” The authors struggle to understand this type of response as our questions related to high-level development models and requirements capture methods rather than specific details of implementation of tools or tests. We can only surmise that the tool providers who responded in this way either lack confidence in their own products or believe that they are using innovative development techniques which no other developer has considered.

2. Principles of ISO 17025

Before examining the concept of validation more closely, it may be helpful to review some of the principles which underpin ISO 17025 which are embodied in the earlier version and which have influence its use in “non-forensic”

63 organisation such as those carrying out calibration of tools or testing of chem-
64 ical compounds or metal alloys.

65 Gravel[3], writing in 2002 about the 1999 version of ISO 17025 described
66 8 principles which were embodied within the standard as:

67 Capacity Concept that a laboratory has the resources (people
68 with the required skills and knowledge, the environment
69 with the required facilities and equipment, the quality con-
70 trol, and the procedures) in order to undertake the work and
71 produce competent results.

72 Exercise of responsibility Concept that persons in the organisa-
73 tion have the authority to execute specific functions within
74 the overall scope of work and that the organisation can
75 demonstrate accountability for the results of the work.

76 Scientific method Concept that the work carried out by the or-
77 ganisation is based on accepted scientific approaches, prefer-
78 ably consensus-based, and that any deviations from accepted
79 scientific approaches can be substantiated in a manner con-
80 sidered generally acceptable by experts in that field.

81 Objectivity of results 1. Concept that the results produced
82 within the scope of work of the organisation, are mainly
83 based on measurable or derived quantities.

84 2. Concept that subjective test results are produced only by
85 persons deemed qualified to do so and that such results are
86 noted as being subjective, or are known by experts in that
87 field of testing to be mainly subjective.

88 Impartiality of conduct Concept that the pursuit of competent
89 results through the use of generally accepted scientific ap-
90 proaches is the primary and overriding influence on the work
91 of persons executing tests - all other influences being con-
92 sidered secondary and not permitted to take precedence.

93 Traceability of measurement 1. Concept that the results pro-
94 duced, within the scope of work of the laboratory, are based
95 on a recognised system of measurement that derives from
96 accepted, known quantities (SI system) or other intrinsic or
97 well-characterised devices or quantities.

98 2. Concept that the chain of comparison of measurement
99 between these accepted, known quantities or intrinsic de-
100 vices or quantities, and the device providing the objective
101 result, is unbroken for the transfer of measurement charac-
102 teristics, including uncertainty, for the whole of the mea-
103 surement chain.

104 Repeatability of test Concept that the test which produced the
105 objective results, will produce the same results, within ac-
106 cepted deviations during subsequent testing, and within the
107 constraints of using the same procedures, equipment and
108 persons used during a previous execution of the test.

109 Transparency of process Concept that the processes existent
110 within the laboratory producing the objective results, are
111 open to internal and external scrutiny, so that factors which
112 may adversely affect the laboratory’s pursuit of objective
113 results based on scientific method, can be readily identified
114 and mitigated.

115 With the exceptions of Capacity and Exercise of responsibility, these prin-
116 ciples establish a need to show, not just that a chosen method satisfies re-
117 quirements for an intended use, but that the method is fundamentally correct
118 or sound, and satisfies broader ranging technical requirements.

119 From our reviews of both the 2005 and 2017 versions of ISO 17025, it
120 appears that these principles have been retained in the most recent versions
121 of the standard.

122 **3. Application of ISO 17025:2005 to “non-forensic” disciplines**

123 A regularly voiced criticism of ISO 17025 is that it is, as its title suggests,
124 intended for Testing and Calibration laboratories. In order to understand
125 how ISO 17025 is applied in these “non-forensic” organisations, and to de-
126 termine if or how it is applied differently in a forensic context, the authors
127 carried out a review of publicly available accreditation records.

128 The United Kingdom Accreditation Service (UKAS) maintains a register
129 of accredited bodies [4] which is open for public inspection. The entries in
130 this register include detail of each test for which a body has been accredited,
131 giving a brief description of the method used where appropriate or necessary.

132 Examination of a sample of 100 accredited organisations in a range of
133 “non-forensic” and “non-medical” areas reveals that these organisations ap-
134 ply two approaches to defining the requirements for their accredited process:

135 Physical properties Where precise measurement of physical properties is
136 possible (e.g. for volumetric, force, torque, acoustics), the schedules of
137 accreditations specify, using SI units, the range of measurement possi-
138 ble and tolerances (uncertainty) allowed for that measurement.

139 External standards In other circumstances, where an industry has defined
140 its own standards, the accreditation is based on implementation of the
141 published standard which either defines the range and uncertainty for
142 the measurement, or defines the method itself.

143 In both of these cases, the requirements for the method, and thus its
144 validation, are available in published form (either directly in the schedule
145 of accreditation or in the published standard) and thus can be subjected to
146 independent scrutiny and adopted by others practicing in the same technical
147 field. In fact, the published requirements allow an independent verification of
148 the method to show correctness in the form of conformance to a general set of
149 standardised requirements rather than just conformance to the requirements
150 for a particular use-case.

151 Moreover, the presence of these published criteria allow customers to
152 identify those testing bodies whose methods may satisfy their needs before
153 entering into discussions with the testing body. In effect, the listed require-
154 ments and associated tests become a menu from which the customer and
155 test body can choose the most appropriate way of meeting the customer’s
156 particular needs.

157 4. A Discussion of Validation

158 In many discussions of accreditation against the standard, the concept of
159 “validation of the tool” or even “tool accreditation” is raised by users and
160 vendors as a means to shortening or eliminating the process. To the authors,
161 this hints that there may be some either confusion about the meanings of
162 these terms, or a different use of language in effect. It is, therefore, instruc-
163 tive to consider the software engineering distinction between verification and
164 validation and contrast it with the ISO 17025 view.

165 4.1. ISO 17025:2005 approach to validation.

166 ISO 17025:2005 [2] contains no direct definition of validation but, in ac-
167 cordance with ISO practice, refers the reader to ISO 17000 and ISO 9000
168 for inheritance of relevant definitions. This practice, of relying on definitions
169 found in other standards, is common with the ISO range of standards, but
170 can cause problems for some users as they may perceive a requirement to
171 have access to the defining standard as well as the standard they are trying
172 to implement, or they may rely solely on common usage of the word as op-
173 posed to ISO's stipulative definitions (aka the "Humpty Dumpty" rule³). In
174 practice, ISO provides an Online Browsing Platform [6] (OBP) which allows
175 access to definitions and some other text without further expenditure.

176 Using the OBP, the authors have found that ISO 17000 contains no def-
177 inition of validation. Thus the ISO 9000:2005 [7] definition should be used
178 as this is the most recently published version prior to the publication of ISO
179 17025:2005. This gives the following definition of validation:

180 Confirmation, through the provision of objective evidence, that
181 requirements for a specific intended use or application have been
182 fulfilled.

183 NOTE 1 The term validated is used to designate the correspond-
184 ing status.

185 NOTE 2 The use conditions for validation can be real or simu-
186 lated.

187 and defines objective evidence as

188 Data supporting the existence or verity of something

189 NOTE: Objective evidence may be obtained through observation,
190 measurement, test, or other means.

191 with requirement as

192 need or expectation that is stated, generally implied or obligatory

193 Note 1 to entry: Generally implied means that it is custom
194 or common practice for the organization (3.3.1), its customers

³"When I use a word, it means it means just what I choose it to mean"[5]

195 (3.3.5) and other interested parties (3.3.7), that the need or ex-
196 pectation under consideration is implied.

197 Note 2 to entry: A qualifier can be used to denote a specific type
198 of requirement , e.g. product requirement , quality management
199 requirement , customer requirement .

200 Note 3 to entry: A specified requirement is one that is stated, for
201 example in a document (3.7.2).

202 Note 4 to entry: Requirements can be generated by different in-
203 terested parties (3.3.7).

204 Note 5 to entry: This definition differs from that provided in
205 3.12.1 of ISO/IEC Directives, Part 2:2004. 3.12.1 requirement
206 expression in the content of a document conveying criteria to be
207 fulfilled if compliance with the document is to be claimed and
208 from which no deviation is permitted

209 This suggests that validation is a demonstration of suitability for a par-
210 ticular use-case, that the requirements for a validated process should be de-
211 rived from the intended use-case and that validation should be the process
212 of obtaining data which shows that a method or process meets those specific
213 requirements.

214 4.2. *Software Engineering approach to verification and validation*

215 In the world of digital forensics we tend to rely on third-party tools which
216 we trust have been produced in accordance with good engineering practices.
217 For the most common analytical tools, this is software which we trust has
218 been correctly specified, implemented and tested. However, the responses
219 to our questions about development models suggest that there is some dis-
220 connect between the tool producers and the way end-users are expected to
221 provide evidence of fitness for purpose. In order to understand how this may
222 have arisen, we turned to a consideration of Software Engineering terminol-
223 ogy to discover if there is a fundamental conceptual difference.

224 In Software Engineering, we commonly paraphrase Verification as “are
225 we building the product right?” and validation as “are we building the right
226 product?”[8]. i.e. verification is a demonstration of the correctness of the
227 product whereas validation is a demonstration of suitability for a particular
228 use. More formally the IEEE Standard Glossary of Software Engineering
229 Terminology[9],states these as

230 Verification

- 231 (1) The process of evaluating a system or component to determine
232 whether the products of a given development phase satisfy the condi-
233 tions imposed at the start of that phase.
- 234 (2) Formal proof of program correctness.

235 Validation

236 The process of evaluating a system or component during or at the end
237 of the development process to determine whether it satisfies specified
238 requirements.

239 For completeness, [9] also defines a requirement as

- 240 (1) A condition or capability needed by a user to solve a problem
241 or achieve an objective. (2) A condition or capability that must
242 be met or possessed by a system or system component to satisfy a
243 contract, standard, specification, or other formally imposed doc-
244 uments.
- 245 (3) A documented representation of a condition or capability as
246 in (1) or (2).

247 These definitions are completely consistent with those found in the ISO
248 and ISO/IEC standards under consideration.

249 Software products should, therefore, be subjected to verification during
250 development - to show that they are correct and complete, and validation
251 post-development to show that they meet the requirements for their intended
252 use-cases. In more common terms, the validation test can be considered to
253 be an acceptance test.

254 In the case of custom software, produced in response to a particular prob-
255 lem, the process of verification could result in validation for that problem. In
256 the case of off the shelf software (e.g. word processors, spreadsheets, common
257 forensic tools), however, verification during the development phases is based
258 on a generic statement of requirements which meets the needs of a perceived
259 customer or a group of idealised customers. It is the responsibility of the
260 customer to ensure that the verified tool provides a valid solution to their
261 problem as part of the procurement and pre-deployment process.

262 It is, thus, entirely possible to verify a product which cannot be validated
263 as it does not provide a suitable solution to the problem under considera-
264 tion (e.g. a custom-built spreadsheet may be completely correctly built but

265 unusable as a presentation package) and it is also possible to validate an
266 unverified product by showing that, despite its inherent flaws, the product
267 satisfies a particular case-specific set of requirements. For example, a cal-
268 culator which always states that $2+2=5$ is unlikely to be verifiable, but can
269 participate in a validated method where the requirement is to calculate that
270 $3+3=6$. Similarly a tool, designed to parse FAT filesystems only, will not
271 parse NTFS. It is therefore, not verifiable for NTFS but can participate in
272 methods which are validated for examination of a FAT formatted filesystem.

273 In the latter case the unverified product cannot be shown to have any
274 utility beyond the limited circumstances for which it is validated.

275 In the former case, however, the verified product may be useful in other
276 situations and the presence of evidence of verification can be used to assist the
277 process of choosing it as a potential solution - i.e. the evidence of verification
278 may show that the validation requirements have already been met during the
279 development process.

280 This depends entirely on the existence of suitable statements of require-
281 ments for both the tool as it was developed and the situation in which it
282 is to be used, and satisfactory evidence that those requirements have been
283 satisfied.

284 *4.3. Implications for method validation*

285 Given that the definitions and usage of validation and verification, as
286 outlined above, appear to be consistent it should, therefore, be possible to
287 use software engineering evidence of verification, as suggested in ISO/IEC
288 27041 [1] as part of the validation of a suitably documented method.

289 **5. Our study**

290 *5.1. Laboratory documentation*

291 In our study, we examined a small randomly chosen set of Standard Op-
292 erating Procedures (SOPs) and Validation plans and records from two ac-
293 credited digital forensic laboratories. The SOPs were written in a format
294 which appears to be based on the SWGDE Model [10] and be consistent
295 with the accepted standard format within forensic science laboratories in the
296 UK. These contain sections detailing Purpose, Scope, Equipment, Limita-
297 tions, Procedure, Processing, Success/Failure Criteria and References. None
298 of these SOPs contained any obvious definitions of technical requirements.
299 Rather they tend to define success in terms of processing completing without

300 any errors being reported, and give a broad area of application in the Scope
301 statement.

302 Validation plans contained some identified requirements, but these were
303 arranged as End User (the Criminal Justice System), Legal (including com-
304 pliance with ISO 17025), Compatibility (output format only) and Ethical.
305 No obvious low-level technical requirements were specified in any of the plans.

306 Validation records showed that validation processes tended to consist of
307 evidence that the process under test produced the same results as the same
308 process run on other equipment or that it produced expected results from a
309 particular test case.

310 The testing thus satisfied the letter of the ISO 17025:2005 description of
311 validation, but may not have achieved the level suggested by the principles
312 in [3], particularly in respect of Traceability and Transparency.

313 This apparent failing is not thought to be a problem for other forensic dis-
314 ciplines whose roots lie in other sciences such as chemistry, physics or biology,
315 where the methods used in forensic laboratories are specific adaptations of
316 well-known methods which are used for other purposes and which have been
317 subjected to rigorous peer-review through publication and extensive use in
318 other work.

319 Digital Forensics, however, has its roots in engineering and is highly re-
320 liant on reverse-engineering of decisions and implementations made by others.
321 Many of these implementations (e.g. hard disc firmware, filesystem imple-
322 mentations, data caching) are not published or reviewed as they are commer-
323 cially sensitive and/or there is no need for the majority of users/customers
324 to have any particular interest in the low-level implementational detail which
325 is of particular interest to a digital forensic examiner or analyst. As a result,
326 it may be considered to be difficult for producers or users of forensic tools
327 to show that the tools are actually correct except by potentially lengthy and
328 costly empirical methods.

329 This is compounded by a fundamental difference in the nature of the way
330 in which off the shelf software (OTSS) is used. In a non-forensic context,
331 OTSS is typically intended to process inputs provided by a user in order to
332 generate a particular output. In this situation, the inputs are known, or can
333 be examined, before the output is seen and thus detection of incorrect results
334 can be simple. In the forensic context, however, examinations start with a
335 source of potential evidence whose contents are unknown. Thus the inputs
336 to the whole forensic process are unknown. Although the user may have
337 some experience of what abnormal outputs look like, this depends entirely

338 on the tool actually producing abnormal outputs or indications of errors.
339 It is entirely possible for a tool to process inputs incorrectly and produce
340 something which still appears to be consistent with correct operation. In the
341 absence of objective verification evidence, assessment of the correctness, or
342 otherwise, of any results produced by a tool relies solely on the experience
343 of the operator.

344 It should also be borne in mind that updates to hardware and software
345 may have no apparent effect on system behaviour as far as a typical user is
346 concerned, but may dramatically change the way in which internal processing
347 is carried out and data is stored. This impacts both on the ability to recover
348 and interpret data and on the behaviour of the tools used to perform these
349 operations.

350 5.2. *Vendor evidence of verification*

351 Our study circulated a questionnaire and received 14 responses from tool
352 providers. Of these, 2 could be considered major providers although one is
353 more focussed on e-Discovery than criminal investigations.

354 The 12 small providers seemed confused about what was meant by cus-
355 tomer requirements with responses including “I’m my own customer”, “Sorry,
356 I don’t understand the question”, “Forums, social media”, “I do not - many
357 potential customers seem utterly bemused why they should be interested
358 at all”. Of the 14, 3 identified the use of JIRA / Confluence /Github as
359 a means of deriving requirements and three others identified Meetings and
360 Communications with end users as the mechanisms used.

361 When asked how they demonstrated that their tool satisfied user require-
362 ments, responses include use of NIST test disc images, use within ISO 17025
363 accredited laboratories, and meetings. Only one of the survey group men-
364 tioned compliance testing.

365 We also, as noted in the introduction, met with considerable resistance
366 from some of the better-known providers when we asked for information
367 about this topic. As a result, we cannot provide objective evidence for any
368 degree of confidence that tool providers are meeting the genuine requirements
369 of the digital forensic laboratories.

370 Customers for the tools have little incentive to consider the technical
371 requirements as it seems possible to obtain accreditation to ISO 17025:2005
372 without them, and most tool providers are either unable or unwilling to
373 provide evidence that they have verified their tools against any customer or
374 technical requirements.

375 6. Transition to ISO 17025:2017

376 The position in respect of accreditation to ISO 17025:2017[11] may be
377 somewhat different as this now contains definitions of validation and verifi-
378 cation which are very similar to those used in ISO 27041 and the software
379 engineering world, viz:

380 **Validation** Verification, where the specified requirements are fit
381 for an intended use

382 **Verification** Provision of objective evidence that a given item
383 fulfils specified requirements

384 Thus validation appears, in the newer version, to be reliant on verification
385 against specified requirements and comparison of those requirements with the
386 requirements of the intended use-case.

387 7. Conclusion

388 Contrary to previous arguments that ISO 17025 [12] is an unwieldy stan-
389 dard for digital forensics because of the complexity of validation, we believe
390 that it can be applied if certain preconditions are met.

391 For ISO 17025 to be successfully applied, the existing understanding of
392 requirements needs to be reconsidered. Rather than relying on the concepts
393 of “customer requirements” [13], where the customer is the customer of the
394 laboratory (i.e. law enforcement agents, lawyers, the criminal justice system
395 etc.) to provide the baseline for method validation, forensic science providers
396 should consider the *technical requirements for their own processes and use*
397 *the* customer requirements as a means of selecting the most appropriate pro-
398 cesses to deploy. This would be consistent with the way other “non-forensic”
399 accredited testing and calibration organisations operate.

400 Within forensic science disciplines we suggest that all labs. will have
401 the same common core technical requirements for generic method types (e.g.
402 in digital forensics, hard disc imaging is a core process, as is extraction of
403 data from devices running specific iOS versions etc.), that these should be
404 established by technical working groups from within each discipline, and
405 documented in agreed international standards which can be maintained for
406 use and development by the community.

407 The requirements contained in these standards can then form the basis
408 of a specification mechanism for methods. Clear identification of the techni-
409 cal requirements vs. the non-technical would allow producers and users to
410 identify priority areas for new tool development.

411 Publication, and public maintenance, of this common set of requirements
412 would also allow transparency in the verification and validation process.
413 Rather than relying on “commercially sensitive” information, which may
414 or may not be correct, it would become possible for all those involved to use
415 the disclosed information and make claims (with appropriate substantiating
416 evidence) based upon it.

417 Furthermore, if the suggestion of ISO/IEC 27041:2015 [1] that processes
418 should be designed to be atomic in nature (i.e. small, single purpose with
419 low coupling and high cohesion to other processes) can be followed, the set
420 of requirements for any one process can be kept to a minimum, resulting
421 in a better defined set of conditions for validation and an elimination of
422 revalidation being triggered by changes elsewhere in the process. All the
423 methods which were volunteered for our study were monolithic in nature
424 and contained a high degree of repetition of tightly coupled (by virtue of
425 being included in each SOP) initial process stages (e.g. retrieval of physical
426 items from an evidence store) before progressing to the unique elements of
427 the process.

428 **8. Existing related work**

429 *8.1. Introduction*

430 Since starting the original project, we have been made aware of some
431 projects which may provide, at least in part, some of the missing require-
432 ments, specifications and evidence of correctness. A brief review of two of
433 these, in the context of our analysis and proposals, is given below.

434 *8.2. NIST/DHS Computer Forensics Tool Testing*

435 The National Institute for Science and Technology (NIST) and the Dept.
436 of Homeland Security (DHS) have started some of this work in their Com-
437 puter Forensics Tool Testing programme [14] (CFTT). In this project, a steer-
438 ing group defines the requirements for particular tool functions and NIST
439 then tests tools against the resulting specifications. At the time of writing,
440 the coverage is somewhat limited, concentrating on a few areas which may

441 be particularly common in investigations, but a good range of tools has been
442 considered and an online catalogue of tools and results has been produced.

443 The Federated Tool Testing project as a sub-project of this initiative may
444 be a particularly useful model as it makes available a test suite which can
445 be used by anyone who wishes to test tools against the requirements already
446 defined by the project and share their results.

447 It is unclear, however, how the programme's priority areas are established
448 or how the requirements are, themselves, validated at as this part of the
449 process does not appear to be documented. It is also noteworthy that the
450 requirements are purely at the tool level rather than the broader method
451 level. This may result in an undue emphasis on producing requirements for
452 existing tools, at the expense of producing requirements which have not yet
453 been satisfied but which should be considered high priority as they reflect an
454 emerging real problem area.

455 We also suggest that a broader consideration could create opportunities
456 for better tool integration (i.e. improved exchange of data between tools and
457 better cohesion for improved process flows) as well as improved concordance
458 with external requirements such as legal issues.

459 *8.3. SWGDE guidance on testing and validation*

460 The Scientific Working Group on Digital Evidence (SWGDE) has issued
461 a number of documents which are intended to assist in the design, imple-
462 mentation and validation of methods for digital forensic processes. Of these,
463 the two which appear to have most direct application to the area we are
464 investigating are

- 465 • SWGDE Recommended Guidelines for Validation Testing [15]
- 466 • SWGDE Minimum Requirements for Testing Tools used in Digital and
467 Multimedia Forensics [16] (At the time of writing, this document was
468 in draft form and had been issued for consultation).

469 The SWGDE validation guidance[15] states that

470 Validation testing should be applied to all tools, techniques and
471 procedures

472 and further that

473 Tools, techniques and procedures, which, by virtue of their widespread
474 use, duration of use, and acceptability by the larger informa-
475 tion technology community, are generally acknowledged as reli-
476 able and trustworthy. Consideration may be given to the general
477 acceptance of a tool, technique, or procedure in the determination
478 of whether validation is required.

479 . The latter paragraph appears, to some extent, to contradict the former.
480 In our experience, it seems that this is generally interpreted to mean that
481 something which is in widespread use may be considered reliable.

482 We argue that this is not the intent of the “general acceptance” statement.
483 In part, this is because of the presence of the phrase “larger information
484 technology community” which is a clear indication that the tools, techniques
485 and procedures under consideration are of a more general-purpose nature
486 than the specialist tools deployed in an investigative context. Spreadsheets,
487 word processors, email programs etc. may generally be considered acceptably
488 reliable because they have minimal impact on evidential product and, should
489 they prove to have an error, the sheer number of users worldwide means that
490 it is likely to be detected and documented relatively quickly.

491 More importantly, however, if this general acceptance principle is allowed
492 to apply to commonly adopted “forensic” tools, techniques and procedures it
493 has the potential to result in bad evidence. If the tool, technique or procedure
494 has not been subjected to independent scrutiny (e.g. through peer-reviewed
495 publication or properly evidenced validation testing) there is insufficient ev-
496 idence that it does work correctly. As we note above, digital forensics relies
497 heavily on reverse engineering in order to process and interpret data. At
498 the level that most users operate, it does not have sufficient foundational
499 scientific principles to allow a reversion to first principles to be applied in
500 order to demonstrate correctness. There is always likely to be some doubt
501 or uncertainty about the way the data is being processed and interpreted.
502 This can be reduced only through production of evidence of correctness and
503 adequacy through appropriate software engineering methods, such as testing.

504 Note: we do not see this as a flaw in the SWGDE guidance, but rather
505 in the way that a large part of the community has chosen to interpret this
506 particular recommendation. It should be noted that similar phrases appear
507 in other guidance and, in our experience, are similarly interpreted.

508 The remainder of this document gives a high-level overview of the devel-
509 opment of a testing procedure which, if underpinned by well-defined require-

510 ments which allow the identification of appropriate test cases could result in
511 good evidence of validation and identification of boundary cases for methods.

512 The tool testing guide[16] is more detailed in its recommendations and
513 gives advice about specific tool types and the conditions which should be
514 considered for their testing. Again, however, it makes little reference to
515 using a well-defined set of requirements to assist in the identification of test
516 cases. It does acknowledge that the testing proposed is purely a minimum
517 and that organisations should consider their own particular requirements.

518 It is our view that evidence of testing, produced in the recommended
519 way, could be applied as an adjunct to method validation, providing the re-
520 quirements are properly defined and documented. It should be remembered,
521 however, that tool testing alone is unlikely to be produce the evidence of
522 validation required by either ISO 17025[2][11] or ISO/IEC 27041[1], unless it
523 can be clearly shown that the method is wholly and solely implemented by
524 the tool (see Figure 1).

525 9. Final thoughts

526 While the NIST and SWGDE projects outlined above may start to pro-
527 vide the type of evidence that is necessary to demonstrate that a method is
528 valid, the potential lack of transparency in the requirements definition pro-
529 cesses introduces another element of uncertainty. i.e. if the requirements
530 cannot be shown to be correct, can tests based on those requirements show
531 correctness? This can, to a large extent, be addressed by adopting the “non-
532 forensic” accredited organisation model of using publicly available agreed
533 standard specifications/requirements and/or methods which can be subjected
534 to external independent scrutiny.

535 It also be useful to engage in a more open process, similar to those pro-
536 posed for use in the specification and testing of safety-critical systems [17].

537 [1] ISO/IEC, ISO/IEC 27041:2016 guidance on assuring the suitability and
538 adequacy of digital investigation method (2016).

539 [2] ISO, ISO 17025:2005 general requirements for the competence of testing
540 and calibration laboratories (2005).

541 [3] J. Gravel, Principles behind the requirements of iso 17025, online at
542 http://www.cala.ca/ISO-IEC_17025_Principals.pdf, 2002. Last accessed
543 25th April 2018.

- 544 [4] UKAS, Directory of accredited organisations, online at
545 [https://www.ukas.com/services/other-services/directory-of-accredited-](https://www.ukas.com/services/other-services/directory-of-accredited-organisations/)
546 [organisations/](https://www.ukas.com/services/other-services/directory-of-accredited-organisations/), 2018. Last viewed 4th June 2018.
- 547 [5] Rev. Charles Dodgson (Lewis Carroll), *Through the Looking Glass*,
548 1872.
- 549 [6] ISO, ISO online browsing platform, online at
550 <https://www.iso.org/obp/ui/>, 2018. Last accessed 13th August
551 2018.
- 552 [7] ISO, ISO 9000:2005 quality management systems – fundamentals and
553 vocabulary (2005).
- 554 [8] B. W. Boehm, Verifying and validating software requirements and design
555 specifications, *IEEE Softw.* 1 (1984) 75–88.
- 556 [9] IEEE, Ieee standard glossary of software engineering terminology, *IEEE*
557 *Std 610.12-1990* (1990) 1–84.
- 558 [10] Scientific Working Group on Digital Evidence (SWGDE), SWGDE
559 model standard operation procedures for computer forensics, online
560 at [https://www.swgde.org/documents/Current Documents/SWGDE](https://www.swgde.org/documents/Current Documents/SWGDE QAM and SOP Manuals/SWGDE Model SOP for Computer Forensics)
561 [QAM and SOP Manuals/SWGDE Model SOP for Computer Forensics](https://www.swgde.org/documents/Current Documents/SWGDE QAM and SOP Manuals/SWGDE Model SOP for Computer Forensics),
562 2012. Last viewed 5th June 2018.
- 563 [11] ISO, ISO 17025:2017 general requirements for the competence of testing
564 and calibration laboratories (2017).
- 565 [12] P. Sommer, Accrediting digital forensics - what are the choices?, *Digital*
566 *Investigation* (2018).
- 567 [13] International Laboratory Accreditation Cooperation, ILAC
568 G19:08/2014 modules in a forensic science process (2014).
- 569 [14] National Institute for Science and Technology (NIST),
570 Computer forensics tool testing programme, online at
571 [https://www.nist.gov/itl/ssd/software-quality-group/computer-](https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt)
572 [forensics-tool-testing-program-cftt](https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt), 2018. Last viewed 13th August
573 2018.

- 574 [15] Scientific Working Group on Digital Evidence (SWGDE), SWGDE Rec-
575 ommended Guidelines for Validation Testing (Version 2.0) (2014). Last
576 accessed 13th August 2018.
- 577 [16] Scientific Working Group on Digital Evidence (SWGDE), SWGDE Min-
578 imum Requirements for Testing Tools used in Digital and Multimedia
579 Forensics (2018). Draft Version 1.0 dated 9th July 2018. Last accessed
580 13th August 2018.
- 581 [17] L. E. G. Martins, T. Gorschek, Requirements engineering for safety-
582 critical systems: A systematic literature review, Information and Soft-
583 ware Technology 75 (2016) 71 – 89.