

Digital Forensics: Validation and Verification in a Dynamic Work Environment

Jason Beckett
University of South Australia
jason.beckett@postgrads.unisa.edu.au

Dr Jill Slay
University of South Australia
jill.slay@unisa.edu.au

Abstract

Many forensic computing practitioners work in a high workload and low resource environment. With the move by the discipline to seek ISO 17025 laboratory accreditation, practitioners are finding it difficult to meet the demands of validation and verification of their tools and still meet the demands of the accreditation framework. Many agencies are ill-equipped to reproduce tests conducted by organizations such as NIST since they cannot verify the results with their equipment and in many cases rely solely on an independent validation study of other peoples' equipment. This creates the issue of tools in reality never being tested. Studies have shown that independent validation and verification of complex forensic tools is expensive and time consuming, and many practitioners also use tools that were not originally designed for forensic purposes.

This paper will explore the issues of validation and verification in the accreditation environment and propose a paradigm that will reduce the time and expense required to validate and verify forensic software tools.

1. Introduction

Forensic computing has mostly developed out of a demand for service from the law enforcement community [1] and has typically developed in an ad hoc manner [2][3][4] rather than a scientific one. It has since developed into a discipline that crosses the corporate, academic, scientific as well as the law enforcement domains and it is developing both as a discipline and a forensic science [5][6][7].

With its embryonic development the discipline is facing some of its biggest challenges over the next few years with the move to bring the field inline with other established forensic disciplines. Compliance with ISO 17025 [8] laboratory accreditation is becoming the main method of achieving this goal.

Accreditation brings structure and organization with procedures, documentation and testing. One of the main issues that accreditation brings is the validation and verification of test methods. In a dynamic technological environment, the subject matter of tests (the evidence) changes at such an exponential rate that forensic tools are modified regularly in order to keep up. Mohay [9] identifies the problem in the context of the uptake of new forensic tools and the expense of producing high quality test results.

One of the other issue facing modern specialists with validation and verification is the diversity of tools because of the inability of an individual tool to meet all the needs of a particular investigation [10][4]. The other problem faced is that not all tools used by specialists were designed originally with the forensic process in mind, instead developed to meet the needs of particular interest groups, such as filesystem drivers, operating systems, Indexing engines, etc.

It is the assertion of this paper that there is a fundamental solution to developing a validation and verification model and that is to remove the necessity for developing individual tests for tools and provide a system where neutrality and tool independence can be achieved through a deterministic set of references.

2. The current scientific environment

The connotation of 'forensic' infers a scientific approach and the basis of this scientific approach is scientific method. In order for the discipline to adopt a scientific framework there needs to be scientific method.

The most pressing requirement in this discipline for law enforcement is the 'need for speed' [11] that is, the increase in case load, from the increase in the amount of data requiring examination, is making it more difficult to obtain results in a timely manner. This burden of work and the need to verify test equipment

due to accreditation puts high burdens on examiners and laboratories. The quality of results or the “trustworthiness” of evidence, as described by some authors, is of paramount importance given the forensic (for court) context of the discipline. The quality is dependant on the scientific application of the process, the analysis and the correct utilization and functioning of the forensic tools.

The current ability of law enforcement, the main practitioners in this field [1], practically to apply academic, or even scientific responses to this discipline is of some concern. A major survey project conducted by the National Institute of Justice [12] illustrated that more than 58% of Agencies in the United States still did not have digital evidence policies. This same survey also showed that only 57% of agencies required specific training to duplicate, examine and analyze evidence and more than 70% of Practitioners had no or minimal (less than a few hours) of training in this discipline. These statistics alone are of concern and cement the assertion that law enforcement has a way to go to meet minimum standards for a scientific discipline. There has been no study that could be found that identifies the situation in the corporate or private sector. Anecdotal evidence suggests the situation is no different and may be considerably worse.

One of the tenets of scientific method is the principle of reproducibility. This ability to test and accurately reproduce results is also of concern to the digital forensic community. In most cases reproducibility is achieved in the discipline either by using the same tool or by cross validation of forensic tools, that is, producing the same result with two different tools. These methods are sound methodologies in the context of Judicial or scientific reproducibility but both have a major flaw inasmuch as they do not deal with what happens when the tools are incorrect. We have met the tenet of reproducibility of the process, that is we can reproduce the result of a tool or test, but not necessarily the principle of reliability.

There have been many attempts to define the field, like the broad definition introduced by McKemmish [13] an Australian practitioner in the field, who postulates the four main concepts of identification, preservation, analysis and presentation, which has been prevalent in the field and often cited. Varney [14] applies the context of computer science to the “investigative legal process” therefore introducing the concept of forensic, in which Mark Pollitt, one of the industry’s longest serving practitioners, generalizes on this “information of probative value stored or transmitted in digital form” [15] Brian Carrier another

academic commentator in this discipline attempts an all-encompassing definition [16]

“The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”

Needless to say that with all these definitions and the many more in a similar vein ([18][19][20][21][22][23],etc) form the nexus between digital data, jurisprudence and science.

A variety of authors have discussed these descriptions in great depth or extrapolated their own model of the discipline [4][24][25] or simply listed the pros and cons of many models [26][6] in a call for more work to be done.

In addition to the frameworks mentioned previously, the use of digital forensics in investigations with a view to defining a common response to evidence, has also been looked at from a range of angles, including forensic readiness [27] in investigations, military operations [18] or processes in investigations [28][29]. There are also a number of frameworks and guidelines developed from authoritative bodies, such as the Department of Justice [30] and the Association of Chief Police Officers in the UK [31]. None of these models specifically discusses the validation of tools and processes and instead look at the reliability of the evidence. Accreditation calls for the validation and verification of the tools.

3. ISO 17025 Laboratory Accreditation

This international standard is intended to specify the general requirements for the competence to carry out test and/or calibrations, including sampling. It encompasses testing and calibration performed by the laboratory using standard methods, non-standard methods, and laboratory-developed methods [8]. A laboratory complying with this standard will also meet the quality management system requirements of ISO 9001.

The standard details many requirements for a laboratory to comply with including;

- Management requirements
- Document Control
- Subcontracting tests and calibrations
- Service to the customer

- Corrective action
 - Prevention actions
 - Internal audits
 - Measurement traceability
- and many others.

The subject of this paper relates to the contents of Section 5.4 “*Test and calibration methods and method validation*” of the standard. It is important to note that there is a general misconception that a user can rely on testing conducted by another organization. For example The National Institute of Standards and Testing (NIST) [32][33][34][35][36] has produced a number of detailed validations for write blockers, and forensic imaging software. This testing does not infer that all write blockers and imaging software are valid; it still requires a user to verify their tools work in their laboratory under their conditions. The reason for user verification is illustrated in the following scenario;

Write blocker brand ‘X’ from company ‘Y’ passes all the tests conducted by a testing agency. Laboratory ‘A’ purchases a number of the ‘X’ brand write blockers. It is possible for any one of the following errors to occur;

- A manufacturing fault in construction sees random data written to your target drive. (probably detectable during usage)
- The power rating of the device when used in your country causes an intermittent fault that allows writing to occur (may not be detectable until it is too late)
- The write blocker sustains internal damage that causes it to misread data, and as all reading processes go through the write blocker a hash analysis will return a valid hash. That is, what is read through the device (the incorrect data) is matched by the hash analysis program that receives the same read data through the faulty device therefore saying the data is valid.

Testing may not highlight every error, but will lead to a measure of reliability. The standard takes this into account and in Note 3 of 5.4.5.3 states that the validation is a balance between costs, risks and technical possibilities. Section 5.4.5.2 also may states that a validation only needs to be as extensive as is necessary to meet the needs of the given application or field of application.

NIST have conducted and documented many tests related to devices or software used to acquire electronic evidence. Many of these tests looked at a

wide variety of scenarios, such as damaged disks, odd sector drives, etc. Many of these items are never encountered by a typical examiner and therefore are not required to be repeated. The implications of the need for user testing are exemplified in the NIST testing, but the need to test the complete regime is not qualified.

4. Validation and verification

Validation and verification of the discipline is a difficult task requiring a structured framework [37][38] and only the outcomes are defined in ISO 17025. Craiger et al [39] make the distinction that a single body could not possibly test and evaluate all forensic software, due to the ‘*sheer pace of change*’. This presents unique problems with the discipline since this dynamic change is not found in other forensic disciplines such as fingerprint examination, and DNA testing. While the scientific underpinnings of these disciplines do not change over time there is a development of finer grained testing. In digital forensics, not only does the data created by applications (the evidence) change at a phenomenal rate, but also the tools needed to identify and analyze the data need to change at the same rate.

The development of forensic software tools and high assurance software requires axiomatic proofs in the foundational development of the software. This concept is the foundation of traditional software engineering. The use of formal proofs in non-axiomatic environments becomes more difficult due to the lack of mathematics and instead requires the use of reproducible experiments or tests. The test cases need to be defined, the tests need to be run and the measured results need to be verified. This is the basis for the NIST tests previously described. In this context, the outcomes of the tools are being examined rather than the process of development of the tool. The question can be asked as to why we should not validate the forensic development of such tools also. This statement is valid, and developers should be looking at the validation and verification of the software development lifecycle. As stated earlier, many tools are not developed specifically for the purposes of digital forensics, they are developed for other purposes and applied to the discipline, so this makes it difficult to police.

Validation and verification has been described in a number of contexts; ISO 17025 “General Requirements for the competence of Testing and Calibration Laboratories” describe validation as;

'Validation is the confirmation by examination and the provision of objective evidence that the particular requirements for a specific intended use are fulfilled.'

This standard also states (Note 3 of 5.4.5.3) that *'Validation is always a balance between costs, risks, and technical possibilities'*. This risk management approach is an important concept to note and will be expanded on later in this paper.

The Scientific Working Group on Digital Evidence (SWGDE) [40] take a simplistic view and define validation testing as ;

'An evaluation to determine if a tool, technique or procedure functions correctly and as intended.'

In the software engineering field, Boehm [41] defines validation and verification a little more succinctly;

'Validation: Are we building the right product?'

'Verification: Are we building the product right?'

Taking into consideration all these definitions and keeping in mind the requirements of ISO 17025, validation and verification of forensic tools can be defined in the context of digital evidence by combing some of these descriptions;

'Validation is the confirmation by examination and the provision of objective evidence that a tool, technique or procedure functions correctly and as intended.'

'Verification is the confirmation of a validation with a laboratories tools, techniques and procedures'.

3. Digital Forensics problems

The complexity of formally describing an entire science needs to start with a review of the literature and a discussion with industry leaders from a diverse range of backgrounds. Attempts in the past have concentrated on the "trustworthiness" of digital evidence, that is the product of the process [17][42], and not the validity of tools.

For this validation and verification model to be developed the discipline needs to be described in sufficient detail so that the discrete functions can be applied to the model. Despite a number of calls for a defined model [7][6] and the various excellent attempts at formally describing components and processes of the discipline [43] [10][44][45][4] there is still no adequate description of any depth of the specific functions of the discipline.

Digital forensics is very much an emerging discipline and has developed in an ad-hoc fashion [2][3][4] without much of the scientific rigour of other scientific disciplines, such as DNA, ballistics, and fingerprints. There have been recent efforts to formalize a definitive theory of Digital Forensics and research dissertations that focus on the process model have started to appear. One major commentator in this field Brian Carrier [43] postulates an "Hypothesis-Based Approach to Digital Forensic Investigation".

There is also research, although not definitive or in-depth, into the validation of the results of forensic investigations (that is, the reliability of the evidence), but very little on the reliability of the tool that produces the evidence. This has been deemed too difficult by a number of researchers [39] due to cost, time and resources. This concept is also prevalent in standards such as ISO 17025 that make the statement (Note 3 of 5.4.5.2) that 'Validation is always a balance between costs, risks, and technical possibilities'. NIST and the SWGDE have realized this fact and have attempted to produce validation methodologies to address the deficiency [40][32]. Both methodologies are broad and offer no conclusive detailed identification of what needs to be tested.

In discussions with practitioners, there has been a heavy reliance on vendors to validate their tools. The vendor validation has been widely undocumented, and not proven publicly, except through rhetoric and hearsay on the bulletin boards of individual tool developers such as Guidance Software (www.encase.com), and Access Data (www.accessdata.com) the main players in this domain. Many published documents in this field discuss repeatability of process with other tools as the main validation technique, but no documented record can be found in the discipline that expands on the notion of two tools being wrong. Gerber and Leeson [46] also postulate that it would be impossible precisely to determine the correct operation of a tool without a "full source code level audit" of the tool.

The emerging problem that practitioners are facing, due to the dynamic nature of technology, is the ability for tools designed solely for forensic purposes to keep abreast of the broad range of technology. In many cases, these practitioners are relying on software that was not developed for forensic purposes, because of either cost or availability, but produces the results that are required for the investigation. Examples include email applications, internet cache examinations, online chat log viewers, etc. Many of these tools are

proprietary in nature and reverse engineering by forensic vendors is not timely enough before new versions of the original product are released.

4. Traditional testing methods

Traditional software and systems engineering development models have placed testing as part of the development lifecycle (See [47][48]) and emerging trends in these fields are putting even greater reliance on testing as part of the development process such as the development of Agile and Extreme Programming.

Traditional research discourse on tool testing in this discipline concerns validation of a tool, that is, all the functions of a tool, and with the failure of a validation of a tool the traditional thinking is to invalidate the tool. In most cases forensic tools are quite complex and provide hundreds of specific functions, of which only a few may ever be used by an examiner. Even trivial testing of all functions of a forensic tool for every version under all conditions, conservative estimates would indicate significant cost.

5. A new paradigm

Given the high cost and time involved in validating a tool and the lack of verifiable and repeatable testing, a new sustainable model is required that meets the need for reliable, timely and extensible verification and validation.

The concept of reference sets is not new and a number of sample sets have begun to appear. An example is the Digital Forensic Tool Testing (dftt) project (www.dftt.sourceforge.net). The dftt project has produced only 12 basic tests at the time of writing. In order for a deterministic suite of reference sets to be established, there needs to be a fundamental mapping of the functions of the discipline as opposed to the previously mentioned process view that has been traditionally discussed. When an extensible model, as opposed to a definitive model, has been established practitioners, tool developers, and researchers are capable of identifying critical needs and target deterministic reference sets.

This paradigm treats the tool or process used to produce valid results, as independent from the mechanism used to validate the tool or process.

If the domain of forensic functions is known and the domain of expected results are known, that is, the range and specification of the results, then the process of validating any tool can be as simple as providing a set of references with known results. When a tool is

tested, a set of metrics can also be derived to determine the fundamental scientific measurements of accuracy and precision. Figure 1 shows this concept diagrammatically.



Figure 1 – Model of tool neutral testing

The theory is if the discipline can be mapped in terms of functions (and their specifications) and, for each function, the expected results identified and mapped as a reference set, then any tool, regardless of its original design intention, can be validated against known elements. This regime of developing reference sets has the added features of extensibility, tool neutrality, tool version neutrality and transparency.

Extensibility: With a defined function, there exists a set of specifications for components that must be satisfied for the result of a function to be valid. That means as new specifications are found they can be added to a schema that defines the specification.

Tool Neutrality: If the results, or range of expected results, are known for a particular function, then it does not matter what tool is applied, but that results it returns for a known reference set can be measured.

Tool Version Neutrality: As a tool naturally develops over time, new versions are common, but the basic premise of this validation and verification regime means that the comments previously described for tool neutrality are also measurable.

Transparency: A set of known references described as a schema are therefore auditable and independently testable.

Each tool can therefore be validated and verified on its merits and the examiner can focus on the results required rather than the domain of all possible functions and all possible specifications.

6. Example

This paradigm expressed best through an example. Keyword searching is one of the most common and basic functions that a practitioner in this discipline will use. This is also one of the most complex implementations in developing a forensic tool. It forms the basis for nearly all of the forensic functions that an examiner will use. A keyword search could be

as simple as looking for a specific word within a file, or looking for a valid email address through a complex regular expression, such as;

```
\b[A-Z0-9._%~]+@[A-Z0-9.-]+\.[A-Z]{2,4}\b
```

(Note: this is a simple example, a regular expression that implements the complete RFC822 is some 6343 characters in length [49]).

The domain of all search functions are discussed later in the paper, for the purposes of this example a simple single keyword search will be used.

Function ‘*Search.keyword*’ will need to take into account the following simplified specification;

Case sensitivity: Is it in upper or lower case, or does it matter). E.g KEywoRd

Fragmentation: Is the keyword located in fragmented disk space, that is does half the keyword physically (at the raw disk level) sit in one sector, while the other part of the keyword sits in another sector physically located elsewhere on a disk.

Compound sentence: Is the keyword surrounded by characters or white space?. E.g. (keyword)

Compound container: Is the keyword located in a container such as a compressed file.

Deleted: Is the keyword in a file that is deleted.?

Unallocated space: Is the keyword located in an unallocated region of the disk?

Slack space: Does the keyword reside at the end of a file, but before the physical end of the sector that the file occupies?

Alternate data stream: Is the keyword in an alternate data stream?

Metadata: Is the keyword located in the metadata of a file or disk, such as a Directory Entry (FAT, NTFS MFT entry, Journal Entry) or OLE data extension?

A tool that fails to find a keyword in a compound container should not invalidate the tool. It should, more importantly be recognized that it fails in that one instance but passes other specified tests. Another scenario occurs when a user is looking for keywords in document files, the fact that a tool does not find the keyword in unallocated space should not be of concern to the analyst.

Another example; Two separate methods for keyword searching using two different tools. A ‘grep’ search over a raw ‘dd’ image (copy) of a filesystem and the use of a forensic tool such as Encase or FTK over the same ‘dd’ image of the filesystem.

The following scenarios are tested;

1. Keyword within a text file.
2. Keyword within a text file in a compressed archive.
3. Keyword as a graphic representation (i.e. not text but an image’.

The hypothesis is both tools or methods should produce the same results for a simple text based keyword search.

grep

If we run a ‘grep’ for the word ‘*Keyword*’ over the ‘dd’ image it would be expected that the following would occur;

TEST 1: PASS - Keyword found in text file.

TEST 2: FAIL - Keyword not found. Reason: the raw ‘dd’ image has no context, that is, grep will treat the ‘dd’ file as a raw data stream and the compressed file would be represented as pure binary data. (note: a mounted image would produce the same results, unless grep was specifically told to mount compressed files)

TEST 3: FAIL - Keyword not found. Reason, as for test 2 the data presented to the grep expression is binary.

Forensic Tool

If we run an automated search for the word ‘*Keyword*’ over the ‘dd’ image it would be expected that

TEST 1: PASS - Keyword found in text file.

TEST 2: PASS - Keyword found in compressed container. Reason: The automated tools gives context to the data, that is, the tool mounts the filesystem in a virtual perspective and if instructed, treats containers such as compressed files in the same way.

TEST 3: FAIL - Keyword not found. No automated forensic tool currently has the ability to arbitrarily provide context to a graphic file. Optical Character Recognition (OCR) may be the only way to adequately identify the keyword.

Comment

In the tests above it may be possible to conclude a range of validation scenarios;

- Grep is a valid tool on raw data files when the data is in a text only file.
- Grep fails on raw files when the data is in a compound file.
- Grep fails on raw files when the data is in a non textual format.

- An automated forensic tool is valid on raw data files when the data is in a text file or a known compound file.
- An automated tool fails on raw data files when the data is in a graphic format.

From these examples, it can be seen that if we know expected results and can measure a tool against these known results we can determine validity. We can also determine the level of validity, that is, match our needs against the results rather than against all results.

Note: These scenarios are trivial and could be compounded by any of the scenarios detailed previously. Indexing engines further compound the problem by adding new complexities, in terms of what is indexed and what is not such as text and binary files.

7. Mapping the Discipline

The digital forensic discipline has been broadly defined in terms of the key *functions Identification, Preservation, Analysis and Presentation* of digital evidence [13]. There are many adaptations of this model, but, fundamentally, the discipline can be described by these four criteria. In the context of validation and verification, Identification and Presentation are skill based concepts, while Preservation and Analysis are predominately process, function and tool driven concepts and are therefore subject to tool validation and verification.

At a Scientific Working Group meeting in Australia in March 2006 for the National Institute of Forensic Science [50], a model was constructed that developed this concept of describing the discipline in terms of functions. The working group agreed to describe the digital forensic component in terms of the two testable classes, that of data preservation and data analysis. These two classes in their broadest definitions describe the science in sufficient detail to allow a model that is useful for accreditation purposes, not only in validation and verification, but also proficiency testing, training (competency) and development of procedures.

Data Preservation in terms of validation and verification was described in terms of four (4) main sub categories, while *Data Analysis* was described in terms of eight (8) categories. Figure 2 is a pictorial representation.

Each sub category of the test classes represents a distinct functional dissection of the discipline.

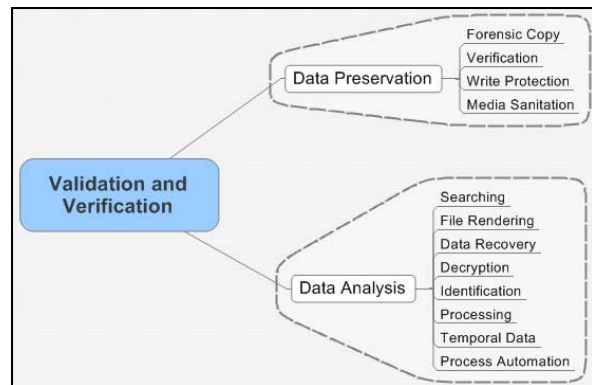


Figure 2 – Validation & Verification top level model

Data Preservation

1. Forensic Copy – represents all methods of producing a verifiable copy of the data. A copy can be as simple as a file or hard disk copy (image), to as complex as a network traffic intercept and a dynamic memory copy. (see figure 3 for a sample functional breakdown for one component of forensic copy)
2. Verification – Numerous methods of verification are used to verify a copy of preserved material and can be tested.
3. Write Protection – There are a wide variety write protection methods including hardware and software that can be tested.
4. Media Sanitation – When preparing for preservation many practitioners prepare media by wiping it; this process too is verifiable.

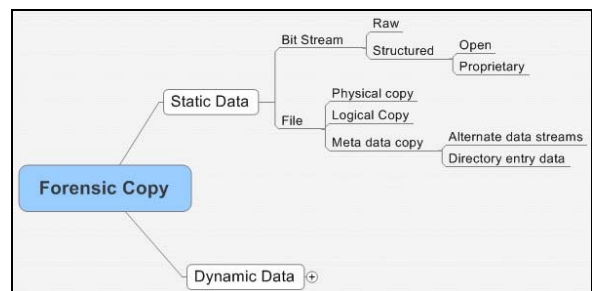


Figure 3 – Forensic copy breakdown

Example

A simplified breakdown of the forensic copy category serves as an example of the depth of categorization of functions. Static data reflects the data that remains constant; that is, data if preserved by two people one after the other, the result should remain constant. An example is a file copy or a forensic copy (Bit stream image) of a hard disk drive or piece of media.

Dynamic data is data that is in a constant state of flux. That is, if dynamic data is preserved and a subsequent preservation undertaken, the resultant copy would be different to the original preservation. For example, preservation of TCP/IP traffic would only exist at the instant that the intercept took place, as is the same with a computers memory which is in a constant dynamic state. A preservation of either traffic or memory could not be repeated with consistent results.

In Figure 3; an example of a proprietary structured bit stream, could be an Encase™ or Expert Witness file format, while a raw bit stream could be a 'dd' image file format.

Data Analysis

1. Searching – The foundational function of the discipline, and includes a variety of testable functions, such as Boolean searches, indexing, soundex searches, etc.
2. File Rendering – Being able to display or render data in an accurate manner is an important contribution a tool makes and can be tested.
3. Data Recovery – This section is not just about recovery of deleted files, but rendering of the filesystem and the recovery of data in unallocated space.
4. Decryption – The application of methods to recover plain text from encrypted data, for example the recovery of keys is testable.
5. Identification – Determination of the type of a file from its data and metadata, such as signature analysis. This too can be validated with known reference data
6. Processing – The processing of data is an especially important function of any forensic tool, such as sorting, reporting and book-marking of data.
7. Temporal Data – The description of time, and rending the temporal components relative to a local context. This can include file date time stamps, metadata, system times, and reference time sources.
8. Process automation – Tying all of the components detailed above together is the predominate function of a tool. How a function operates alone and in unison with other functions can be tested also.

Example

The data analysis component is complex and categorization is diverse. A simplified breakdown of the search function shows the complexity that may be present in the other categories. The testable

components of the search function can be seen as two main categories that of the expressions that are used to search and the targets that are searched. Figure 4 gives the pictorial representation.

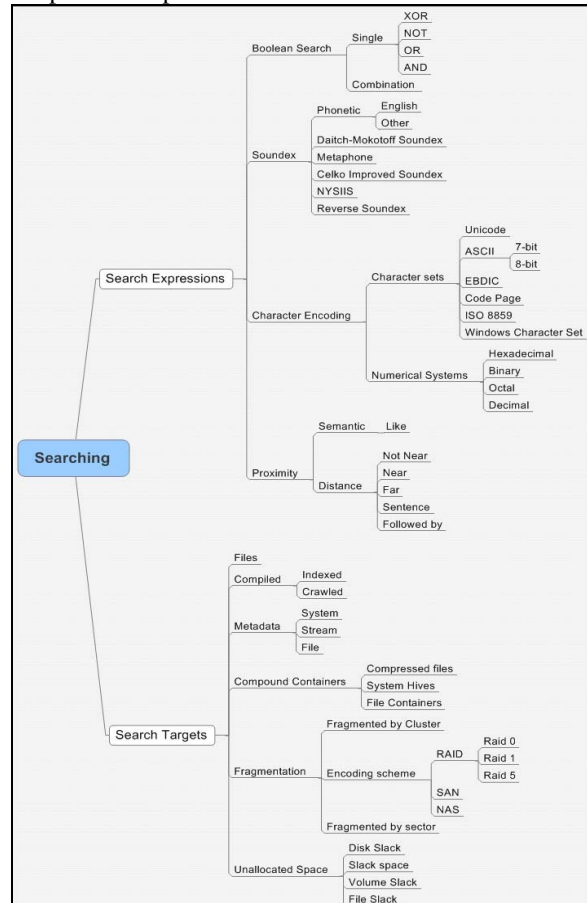


Figure 4 – Searching breakdown

8. Use of Reference Sets

Construction of a reference set for each function, or a consolidated set of references, is now achievable. By individually specifying requirements for each function, we are able to apply metrics to determine the accuracy and precision of the results. That is, we are able to identify known expectations and can compare a tool against these identified components in order to validate a tool. Accuracy is the degree to which the results of the tool being tested match the specification for each of the functions. Precision is the degree to which the results of many test give the same result.

The benefit of a reference set that accurately reflects the specifications of the functions in a variety of measures allows for greater precision in determining the validity of a tool. An example of this is the searching test case introduced earlier. The more search

test cases that reflect the search specifications, (uppercase, fragmentation, compound container, etc) the greater the precision of the test results.

The reference sets can then be applied to a particular search process, as well as any tool that professes to have a search function.

9. Conclusion

The introduction of accreditation into modern digital forensic laboratories has many implications to practitioners in the discipline. The high workload and dynamic environment that practitioners operate in, make it difficult to meet the key requirements of accreditation. The model proposed in this paper identifies a plausible paradigm shift in validation and verification in order to assist in the process.

The mapping of the discipline in terms of discrete functions is the first major component in this paradigm. The individual specification of each identified function will then provide the measure against which a tool can be validated. This allows a validation and verification regime to be established that meets the requirements of extensibility, (the test regime can be extended when new issues are identified), tool neutrality (indiscriminate of the original intention of the tool or the type of tool used), and dynamically reactive (the testing can be conducted quickly and as needed).

In the context of software engineering and the definitions provided by Boehm previously, with this new paradigm we can now comply with the following statements;

- *Is the product valid?*
 - *Are we building the right product?*
- *Can I verify that the product is valid?*
 - *Is the product we built right?*

10. References

[1] Noblett M, Pollitt M, & Presley L. (2000) *Recovering and examining computer forensic evidence*, Forensic Science Communications US Department of Justice Federal Bureau of Investigation Volume 2 Number 4.

[2] Leigland R. & Krings AW. (2004) A formalization of Digital Forensics. *International Journal of Digital Evidence*. Fall 2004, Volume 3, Issue 2.

[3] Etter, B. (2001) *The forensic challenges of e-crime*. Australasian Centre of Policing Research. Publication No.3 October 2001.

[4] Reith M, Carr C, Gunsch G. (2002) An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, Fall 2002, Volume 1, Issue 3.

[5] US-CERT (2005) *Computer Forensics*, United States Computer Emergency Readiness team www.us-cert.gov/reading_room/forensics.pdf visited January 2006.

[6] Broucek V, & Turner, P. (2001). *Forensic Computing: Developing a Conceptual Approach for an Emerging Academic Discipline*. Paper presented at the 5th Australian Security Research Symposium, 11 July 2001. Perth, Australia.

[7] Wilsdon T. & Slay J. (2005) *Digital Forensics: exploring validation, verification & certification* Presented at First international workshop on Systematic Approaches to Digital Forensic Engineering 7-9 November 2005. Taipei.

[8] AS ISO/IEC (2005) ISO 17025 - General Requirements for the competence of Testing and Calibration laboratories. 6th December 2005.

[9] Mohay G. (2005) "Technical Challenges and Directions for Digital Forensics", *Proceedings of the first International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*, IEEE Computer Society, Taipei, 2005. pp2-3.

[10] Bogen C, & Dampier D (2005) "Unifying Computer Forensics Modeling Approaches: A Software Engineering Perspective." *Proceedings of the First international workshop on Systematic Approaches to Digital Forensic Engineering 7-9 November 2005*. Taipei.

[11] DFRWS "DFRWS 2005 Workshop", Digital forensics research workshop, DFRWS, New Orleans, August 17-19 2005, pp 27.

[12] Appel EJ, Pollitt MM. (2005) Report on the Digital Evidence Needs Survey of State, Local and tribal Law enforcement. National Institute of Justice, US Department of Justice

[13] McKemmish, R (1999) *What is forensic Computing?* Trends & Issues in Crime and Criminal Justice No. 118.

[14] Varney T (2000) Computer Forensics. In; Internal auditing, November / December 2000, pg 31-33.

[15] Pollitt M. (2006) Digital Forensics. In; Wecht C and Rago JT (editors) *Forensic Science and Law – Investigative Applications in Criminal, Civil and Family Justice*. CRC Press - Taylor and Francis Group. [Chapter 27]

[16] Carrier B. (2003) Defining Digital Forensic Examination and Analysis Tools Using Abstraction layers. *International Journal of Digital Evidence*. Winter 2003, Volume 1, Issue 4.

[17] Palmer G. (2001) A Road Map for Digital Forensic Research. Technical Report T0010-01, Digital Forensics Workshop (DFRWS). November 2001.

[18] Giordano, J., & Maciag, C. (2002). *Cyber forensics: A military operations perspective*. *International Journal of Digital Evidence*, volume 1 Issue 4 2002.

- [19] Farmer D, Venma W. (1999) Computer Forensic analysis Class Hand outs. www.fish2.com/forensics/intro.pdf. Visited January 2006.
- [20] Mack M. (2003). Electronic Discovery vs. Computer Forensics. New Jersey. Law Journal, 1.
- [21] Patzakis J. (2002) Encase Legal Journal Second Edition. Guidance Software, Pasadena, California. Available from www.encase.com. Visited January 2006.
- [22] Patel A. & O'Ciardhuain S. (2000) The Impact of Forensic Computing Telecommunications. IEEE Communications Magazine pp 64-67.
- [23] Hannan M, Turner P (2003) Australian Forensic Computing Investigative Teams: Research and Competence. Presented to 7th Pacific Asia Conference on I.S., 10-13 July 2003, Adelaide, South Australia.
- [24] Kruse WG, & Heiser JG. (2002) *Computer Forensics – Incident response essentials* Addison Wesley. Boston MA.
- [25] Civie V, Civie R (1998) *Future Technologies from Trends in computer forensic science* IEEE 105-106.
- [26] McCombie S, Warren M. (2003) *Computer Forensic: an Issue of Definitions*. Proceedings of 1st Australian Computer, Network & Information Forensics Conference. 25 November 2003, Perth Western Australia.
- [27] Rowlingson R. (2004) "A Ten Step process for forensic Readiness". *International Journal of Digital Evidence*. Winter 2004 Volume 2, Issue 3.
- [28] Beebe NL, Clark JG. (2005) "A hierarchical, objectives-based framework for digital investigations process. *Digital Investigation* 2005:2, pp147-167. Elsevier.
- [29] Rui bin G, Yun GK, Gaertner M. (2005) Case-Relevance Information Investigation: Binding Computer Intelligence to current computer Forensic Framework. *International Journal of Digital Evidence*. Spring 2005 Volume 4 Issue 1.
- [30] Rui bin G, Yun GK, Gaertner M. (2005) Case-Relevance Information Investigation: Binding Computer Intelligence to current computer Forensic Framework. *International Journal of Digital Evidence*. Spring 2005 Volume 4 Issue 1.
- [31] ACPO (2003) Good Practice Guide for Computer Based Electronic Evidence, Association of Chief Police Officers, from www.nhtcu.org. Visited January 2006. (no longer available from this site)
- [32] NIST (2001) General Test Methodology for Computer Forensic Tools. National Institute of Standards and Technology US Department of Commerce. Version 1.0 November 2001. Available from www.cftt.nist.gov. Visited January 2006.
- [33] NIST (2003a) Software Write Block Tool specification & Test Plan Version 3 September 1, 2003. National Institute of Standards and Technology US Department of Commerce. Available from www.cftt.nist.gov. Visited January 2006.
- [34] NIST (2004a) Digital Data acquisition Tool Specification (Draft 1 of Version 4.0, 4 October 2004. National Institute of Standards and Technology US Department of Commerce. Available from www.cftt.nist.gov. Visited January 2006.
- [35] NIST (2005a) Digital Data acquisition Tool test Assertion and Test plan (Draft 1 of Version 1, 10 November, 2005. National Institute of Standards and Technology US Department of Commerce. Available from www.cftt.nist.gov. Visited January 2006.
- [36] NIST (2005b) Hardware Write Blocker (HWB) Assertions and Test Plan. Draft 1 Version 1 March 21, 2005. National Institute of Standards and Technology US Department of Commerce. Available from www.cftt.nist.gov. Visited January 2006.
- [37] Armstrong C. (2003) Developing a Framework for Evaluating Computer Forensic Tools. Presented at Evaluation in Crime Trends and justice: Trends and Methods Conference in Conjunction with the Australian Bureau of Statistics, Canberra Australia 24-25 March 2003.
- [38] Wilsdon T. & Slay J. (2005b). *Towards A Validation Framework for Forensic Computing Tools in Australia*. Presented at the European Conference of Information Warfare 05, 11-12 July 2005. Glamorgan, Wales.
- [39] Craiger JP, Pollit MM, Swauger J. (2005) Law enforcement and Digital Evidence. In: Bigdoli H (ed) Handbook of Information Security John Wiley & Sons (in Print).
- [40] SWGDE (2004a) Recommended Guidelines for validation testing Version 1. Scientific Working Group on Digital Evidence. July 2004. www.swgde.org. Visited January 2006.
- [41] Boehm BW. (1997) Software Engineering: R&D Trends and Defence Needs. In Sommerville I (2004) software engineering. Addison Wesley. pp 526.
- [42] Hsu ICW, Lai CS (2005) A DCT Quantization-Based Image Authentication System for Digital Forensics. Proceedings of the First international workshop on Systematic Approaches to Digital Forensic Engineering 7-9 November 2005. Taipei.
- [43] Carrier B. (2006) A Hypothesis-Based Approach to Digital Forensic Investigations. Thesis Dissertation, Purdue University. Center for Education and Research in Information Assurance and Security. CERIAS Tech Reprint 2006-06. Purdue University West Lafayette. May 2006.
- [44] Bogen C, & Dampier D (2005a) Preparing for Large-Scale Investigations with Case Domain Modeling. Presented at the Digital Forensics Research Workshop (DFRWS) New Orleans, 2005.
- [45] Carrier B, & Spafford E. H. (2003) Getting Physical with the investigative process. *International Journal of Digital Evidence*. Fall 2003, Volume 2, Issue 2.
- [46] Gerber M, & Leeson J. (2004). Formalisation of computer input and out put: The Hadley Model. *Digital Investigations* 1:214 -224.
- [47] Pressman R. (2004) Software Engineering: A Practitioners Approach. McGraw-Hill Science/Engineering/Math. 6th edition.
- [48] Sommerville I. (2004) Software Engineering 7th Edition. Addison Wesley.
- [49] <http://www.regular-expressions.info/email.html>. Visited 18 April, 2006.
- [50] EESAG (2006) Electronic Evidence Specialist Advisory Group Workshop. National Institute of Forensic Science. Unpublished minutes. March 2006