

Digital Forensics: Exploring Validation, Verification & Certification

Tom Wilsdon¹ & Jill Slay²
Enterprise Security Management Laboratory
School of Computer & Information Science
University of South Australia
{tom.wilsdon}¹ {jill.slay}² @unisa.edu.au

Abstract

Digital forensic teams and laboratories are now common place within Australia, particularly associated with law enforcement and intelligence agencies. The digital forensics discipline is rapidly evolving to become a scientific practice with domain-specific guideline. These guidelines are still under discussion in an attempt to progress the discipline so as to become as solid and robust in its scientific underpinnings as other forensic disciplines. Influential players, practitioners and observers all agree that rigorous standards need to be adopted to align this science with other forensic sciences. How does one assess the scientific nature of digital forensics with so many independent computing and IT elements combined, and what are the outcomes of each assessment method? Solutions are proposed regularly justifying their use but to date no one international or national standard exists. This paper does not propose a solution but rather explores the concept of Validation and Verification (V&V) with particular respect to digital forensic tools. The paper also explores ISO17025 “General requirements for the competence of testing and calibration laboratories” and develops the testing process to satisfy this standard to allow for Australian digital forensic laboratories to be eligible for certification.

1. Introduction

While the views and perspectives portrayed in this paper are predominantly Australian-centric, it is worth noting that no one nation owns, or has conquered from a quality perspective, the digital forensics discipline. The reasons for this are many and varied, and even to some extent unknown, but it is crucial that hurdles to the growth of digital forensics as a mature international scientific discipline are addressed and removed to allow for its development

The production, use and misuse of digital devices are all growing at a phenomenal rate [1]; [2]. For example, the Apple iPod which was introduced during 2001 has now evolved through several generations, hardware configurations and formats and now dominates in its market. This is just one of many examples to a main stream device with large data storage capacity being embraced by countless users and therefore a valid subject of a digital forensic investigation. This kind of data on the take up of digital devices which have a criminal or misuse potential, coupled with results with results from an e-crime study conducted within the UK, suggests that police simply lack the number of skilled or certified police offers to handle the ever increasing load of cases needing investigation [3].

Keeping abreast of technology for digital forensic practitioners is proving to be difficult, not only due to the developments in the technology itself but also in the specific

implementation changes between models of devices. These changes need continual analysis and standard operating procedures necessary to undertake this task need to be developed and maintained. This problem is amplified by the lack of quality standards within the discipline, which could be seen as a neglected family member of the forensic sciences.

It is worth noting the motive for forensic computing is to investigate and present results to a court of law, or for public discussion [4]. Therefore practitioners within the digital forensics discipline have to present results from investigations on digital devices. Within the UK, a group of politicians have questioned the ability of juries to understand and deliver a verdict on complex scientific evidence, such as digital evidence. In this report, the politicians identify the difficulty for juries to quantify the accuracy of a statement by key technical witnesses, providing the ability for a well trained witness to provide information with insufficient scientific foundations. It is acknowledged that a Forensic Science Advisory Council could verify claims made within court to assist with this shortcoming within the current judicial system within the UK [5].

2. Forensic computing authority within Australia

Within Australia, the National Association of Testing Authorities (NATA) provides standards against which verification and validation of scientific processes may be carried out. The forensic science governing body, the National Institute of Forensic Science (NIFS), manages co-ordinates and provides administration for the various existing forensic disciplines. The capacity that NIFS currently has to handle digital forensics, anecdotally, is limited but currently undergoing review so that development of appropriate policies to mandate standardized testing processes may be carried out.

The establishment of digital forensic laboratories within Australia has predominantly been aligned with law enforcement agencies. While these laboratories or teams have worked successfully since their establishment, the discipline is now developing to a stage where the procedures, tools and people must be gauged against a quality and competency framework. The competence testing of the operators and other humanistic elements are beyond the scope of this paper but it is acknowledged that research is being conducted to develop the best processes to complete this aspect of the framework. The validation and verification of forensic tools, principally software, needs to be conducted and opinions vary on the best process for this. There is a general consensus among influential players that a framework must be established to provide the foundations of tool testing [6, 7, 8].

3. Validation & Verification

A model for such a framework has been discussed by expert groups in Australia and the need has been established for a validation and verification model. This is not dissimilar to the IEEE Standard 1012-1998 [9] and IEEE draft P1012/D12 [10]. While these standards were developed to provide guidelines for software and system development, they provide a basis for the digital forensics discipline to adapt for its own requirements. The terms validation and verification have been touted within forensic computing regularly so it is important to understand their meanings; below is the IEEE interpretations of the terms.

‘Validation is the process of evaluating a system or component during or at the end of the development process to determine whether it satisfies requirements. The process of providing evidence that the software and its associated products satisfy system requirements allocated to

software at the end of each life cycle activity, solve the right problem, and satisfy intended use and user needs.'

'Verification is the process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase. The process of providing objective evidence that the software and its associated products conform to requirements for all life cycle activities during each life cycle process, satisfy standards, practices, and conventions during life cycle processes, and successfully complete each life cycle activity and satisfy all the criteria for initiating succeeding life cycle activities.'

4. Forensic sciences

Within Forensic sciences in general are the union of investigative skills within scientific disciplines, and digital forensics is no different. The definition of the particular elements interacting to produce the digital forensics discipline is varied and depends on the author and their background. A practitioner may be more focused on the investigation techniques with an emphasis on computer science skills while an independent observer may perceive law as the main element of a forensic computing investigation. Wilsdon & Slay [8] propose that the individual disciplines and their respective practices can be collectively grouped and then each group evaluated independent of other groups and reassessed upon reconstructing the environment. This allows for a lower level inspection of the individual elements that form the forensic computing discipline but does not allow for an over all audit of the completed discipline at an operational level. Whether this can be achieved is yet to be determined from the publications currently available, but what is readily available is a range of literature which discusses and evaluates components of the computer forensics discipline with individual elements being assessed independently.

Robertson in 1991 presented his personal philosophical viewpoint on the future of forensic science for the period extending 10 years. In the conclusion of this publication states,

'New technologies and improved instrumentation will continue to emerge. Forensic science usually has a lag period before these are adopted into the forensic area, and this is to be expected, given the conservative nature of the legal arena. In the past, however, the lag period has been too long. Forensic scientists need to be quicker to recognize the potential applications to forensic problems and they also need to be able to carry out research aimed at helping to interpret what analytical data means.' [11]

This one quotation summarizes the life cycle of digital forensics thus far. Hannan [12] suggests that digital forensics originated in the late 1980s. As the usage of personal computers increased, along with the uptake of internet connections, digital forensics further developed with prime player being law enforcement. Within Australia the first definition of digital forensics, or forensic computing, was published by Rodney McKemmish in 1999. This publication was timely with other key participants in the area also published their own definitions of the discipline. Hannan (2004) goes about exploring each of the definitions and trying to determine the most suitable for the current context, but for the scope of this paper it is important only to note the date of these publications, 1999, approximately 6 years ago.

While this provides a relevant timeline to determine the progression of digital forensics it is valid to note that Pollitt, a special agent of the FBI, presented a first publication (to the authors' knowledge and only with reference to the public domain) in 1995. So, approximately 10 years ago, the FBI were publicly acknowledging their use

and knowledge of digital forensics and releasing material which propose similar ideas or concepts that today are still desired in the discipline. Pollitt [13] suggests that forensic computing investigations had been active for some period, and led predominantly by a trial and error approach. Furthermore the tools utilized and the types of investigation varied greatly and rapidly but one key appeal would be the development of standards to assist in such investigations. Pollitt noted that although legal differences from jurisdiction to jurisdiction offered substantial difficulty to implement standards the overall discipline would benefit from their introduction.

Now leaping forward 10 years to 2005, have these suggestions been implemented? The short answer is no. Variations of the original recommendations have been presented, but these are not implemented either. In fact, Robertson was frightening accurate describing the time of embracement for new forensic disciplines back in 1991. A final recommendation to his paper was that the future will not be smooth from research and development to implementation and quite simply it will require leadership with the risk of failure [11].

Questions should now be asked such as, who is the leading the digital forensics discipline within Australia, and what is the nature of their organization and the thrust of their approach? How are they addressing the 10 plus years of experience of both local and international practitioners and researchers and, in particular, how are they adopting the recommendations of these pioneers in this field. Within Australia, NIFS is an organization which has enormous expertise in overseeing the other forensic science disciplines and ensures the guidelines of the NATA are implemented to ensure quality management. Should NIFS also be responsible for the development of standards and standard operating procedures to achieve similar governance in digital forensics as other forensic sciences? Is the discipline eligible to be tested against NATA criteria?

ISO7025-1999 [14] outlines the requirements for competence of testing and calibration laboratories within Australia. Forensic laboratories, and equipment, are tested against developed criteria and have to satisfy the extensive requirements outlined within this document to gain accreditation. It is therefore acknowledged digital forensic laboratories are now gearing themselves to seek such accreditation – hence providing possibly the first standard for digital forensics.

Key elements within the ISO7025-1999 document which must be addressed, with particular respect to digital forensics are described in the following sections. These elements are seen as possibly providing the greatest difficulties to laboratories seeking accreditation. It is acknowledged that other requirements may also either be adopted from other disciplines, or created with minimal difficulty from the perspective of the authors.

5. ISO/IEC17025-1999 General requirements for the competence of testing and calibration laboratories

ISO17025 is a standard which can be seen as amalgamation of several other ISO standards, such as ISO9001 and ISO9002. Certification of ISO17025 will provide accordance with these included standards and also International Standards. By achieving certification against ISO17025 this demonstrates that a laboratory is competent to produce technically valid data and results.

As with all testing and accreditation procedures fundamental requirements exist, such as documentation. Within forensic science accreditation the documentation is clearly specified and details the models and standards required. ISO17025 extensively details the requirements, providing insight and direction which should be used as the skeleton of the documentation of

the testing procedures. The challenges introduced in relation to documentation are factored around the categorizing of technical requirements, section 5 of ISO17025.

Technical requirements call for thorough assessment and an interpretation of the implications of all factors that may bear consequence upon results gathered. Such factors include human factors, equipment, measurements traceability, test and method validation, and environmental conditions.

The representation of environmental conditions poses significant difficulties since most of the testing of digital forensic tools is carried in the “environment” of a specific computer. While the specifications of the hardware utilized and software installed on the machine may describe the configuration and physical attributes of the environment it does not detail the actual operations to the level of other forensic sciences. The computer environments imposes a layer of abstraction which is hard to snapshot, detail and recreate and therefore increases the likelihood of introducing a random process which may impact the validity and replicability of the results gathered.

The IEEE draft standard for Software Verification and Validation [10] explores the concept of the differing input variables which may impact on the V&V process. The document categorizes the four main inputs as Environment, Operators, Hardware and other Software and explores the difficulties that each introduces to the documentation process.

To determine, measure and document the impact that the operating system, along with other software, has will provide a major difficulty for those seeking accreditation. Whittaker [15] attempted to describe the impact of the software on the host system interacting with particularly software. This publication demonstrated that well developed software is deterministic in isolation, but the ability of such software to be executed continuously and produce the same results was greatly affected by the other software on the system. Further adding to this problem was the fact that the impact was not consistent but rather intermittent and varying providing an even greater element of entropy which cannot be accounted for.

ISO17025 allows for preventative action to be taken if such procedures will ensure valid results. It describes such pro-active measures to allow for either use of a tool/device with a known error which can be neutralized by an operator rather than the blanket discounting such a tool/device.

Such an approach is an important feature of the proposed framework by Wilsdon & Slay [8] where a requirement-based validation is performed on individual functionality of the software package rather than treating the package as a single entity. By validating each of the specific functions, this allows for a complex collection of tools to be partially utilized for active investigations rather than waiting for the complete validation of the complete set. Wilsdon & Slay [8] also highlight that the major forensic software utilized within Australian law enforcement affiliated digital forensic laboratories is packaged based, justifying such an approach. Furthermore the cost of purchasing such software is so great it would be infeasible to discount an entire package due to a single or small group of functions failing validation.

If intermittent or indeterminable errors do exist it is allowed within the ISO17025 standard within section 5.4.5.3. It states

‘The range and accuracy of the values obtainable from validated methods as assessed for the intended use, shall be relevant to the client’s needs.’

The National Institute of Forensic Science Computer Forensic Tool Testing program methodology allows for such a measure to be recorded during the validation process (NIST). Wilsdon & Slay [8] acknowledge the benefits of such a methodology and the development of reference sets to examine the ability of digital forensic tools to work correctly even if this is not comprehensive in the execution of its function. Within an Australian context, Broucek & Turner [16], classify the three main types of environments that forensic computing may be

utilized as criminal, illegal and inappropriate behavior. Each of these classifications could be seen as setting the investigation needs as each category of investigation has different legal requirements to achieve admissibility of results in court. In further publications by the authors, they explore the hierarchy of the environments defining that if the criminal requirements are satisfied then so to be illegal and inappropriate requirements. If illegal requirements are met then inappropriate requirements are satisfied but criminal will not. Therefore it is expected that the requirements of any validation framework would ensure criminal environment requirements to be satisfied, therefore satisfying all three of these environments.

If a digital forensic tool is determined to fail against the criminal model and hence fail validation, it may justify subsequent validation attempts against the lower requiring environments.

A key attribute of ISO17025 is the assurance of quality for test results, section 5.9 of the document. It ensures results can be recreated by following the documentation of the initial testing procedure, and also allowing for additional testing via comparison. In this sense, a validation and verification framework would accommodate this assurance by endorsing a central authority to initially validate a digital forensic tool and then have this result verified by individual laboratories prior to use. If differences are detected, it then must be determined how and why these differences have been introduced, and the question asked whether this feature can be assessed as variation which can be accounted for due to the variables in the computing environment, as described previously, such as software or other environmental factors. If this is not the case, then a policy should exist where the validation is revoked until revalidation is performed to assure the quality of the validation process.

Final requirement of ISO17025 to be highlighted within this publication are the reports generated from this process. As mentioned previously, the documentation process must be thorough and of a specified standard and the compilation of results and other documentation must adhere to the same quality. Within the standard, a statement of compliance/non-compliance with requirements and/or specifications will be issued to signify that the outcome is the result of a quality process. Other information which maybe collated with such a document includes the limitations and or uncertainty of the tool being evaluated.

An example may be that a tool works correctly with the detection of keywords but fails to locate keywords where they are dispersed across different sectors of the hard disk drive. While this does not affect the validity of the tool, it displays a limitation which may provide a result which is not comprehensive when utilized in a particular context.

Inclusion of the testing procedure documentation is essential along with any reference sets developed to validate a tool. This is of particular importance in the context described earlier with centralized validation and independent verification so the same tool can be tested within separate environments to generate the same results. Inclusion of this documentation also allows for a more economical verification for individual laboratories as the majority of documentation is provided with minimal modification to describe their environment and verification process.

6. Discussion

Digital forensic laboratories are seeking ISO17025 accreditation. Currently such laboratories need to address all components within the standard, therefore reproducing material which is common to all laboratories utilizing the same tools. If a centralized body, such as NIFS, began validating digital forensic tools then the requirement for such laboratories would be reduced significantly. The needs for standards and certification provide a level of assurance

that motivate acceptance as a mainstream discipline within the judicial process and associated investigations.

Without an adoption of the ISO17025 standard digital forensics does pose the risk of entering into a crucial era with minimal guidance and possibly being destined to move very slowly, or in circles, until some central authority is established.

If it is agreed that ISO17025 is in fact not the appropriate standard to be used to certify laboratories, operators and tools then it is essential that an appropriate body develops a standard addressing the many highly- specific requirements associated with digital forensic laboratory investigations. For this to occur, a respected organization should be appointed to oversee the scientific progress of the discipline and this should occur immediately.

6. Conclusion

Digital forensics is at a cross road in its development. The cross road offers several paths forward, some more promising than the others. Some of these roads offer a standardized and scientific approach to forensic computing investigations and others offer possibilities of a tool driven or precedent based approach to investigation. Some provide guidance and governance by an independent authority offering a wealth of forensic science knowledge and others do not. It is essential to get leaders within the digital forensics together to determine which road the discipline should take.

Lessons can be learned from international projects which have undertaken similar processes. The benefits of international bodies linking researchers and practitioners not only builds the structure of the digital forensics discipline but also allows that if the validation process already undertaken overseas can be verified, then the results can be assumed within Australia – this needs further exploration but does provide a major kick start for the strengthening of the discipline.

7. References

- [1] Grabowski P (1998) "Crime and technology in the global village." Presented at Internet Crime, 16-17 February 1998. University of Melbourne, Victoria
- [2] Etter, B. (2001) "The Forensic Challenges of E-Crime." Australasian Centre for Policing Research.
- [3] EURIM – IPPR (2004) "Supplying the Skills for Justice: Addressing the needs of law enforcement and industry for investigatory and enforcement skills." [online] <http://www.eurim.org>
- [4] AAFS. (1996) "What is Forensic Science?" [online], American Academy of Forensic Sciences, <http://www.aafs.org/>
- [5] Sherriff, L. (2005). "Science too hard for juries." [online] The Register, <http://www.theregister.co.uk> accessed 27 May 2005.
- [6] Meyers, M. & M. Rogers. (2004) "Computer Forensics: The Need for Standardization and Certification.". *International Journal of Digital Evidence*, 3(2), 2002.
- [7] Giordano, J. & C. Maciag. "Cyber forensics: A military operations perspective." *International Journal of Digital Evidence*, 1(2), 2002.
- [8] Wilsdon T. & J. Slay. (2005). "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.
- [9] IEEE. (2004) "Draft Standard for Software Verification and Validation IEEE P1012/D12." 12 September, 2004.
- [10] IEEE. (1998) "IEEE Standard for Software Verification and Validation IEEE Std 1012-1998." 20 July 1998.
- [11] Robertson J. (1991). "The Future of Forensic Science." Presented at the Asia Pacific Police Technology Conference, 12-14 November 1991. Canberra, Australia.
- [12] Hannan, M. (2004). "To Revisit: What is Forensic Computing?" Presented at the 2nd Australian Computer, Network & Information Forensics Conference, 25 November 2004. Perth, Australia.
- [13] Pollitt, M. (1995). "Principles, Practices and Procedures: and Approach to Standards in Computer Forensics." Presented at the Second International Conference on Computer Evidence, 10-15 April 1995. Baltimore, Maryland, United States of America.

- [14] AS ISO/IEC 17025 (1999). "General requirements for the competence of testing and calibration laboratories." 21 December 1999.
- [15] Whittaker, J. A. (2001). "Software's Invisible Users." IEEE Software, 84-88.
- [16] Broucek, V., and P. Turner. (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.