Forensic Computing Training, Certification and Accreditation: An Australian Overview

Matthew Simon, Jill Slay

Centre of Excellence in Defence and Industry Systems Capability (CEDISC),
Defence and Systems Institute, University of South Australia,
Mawson Lakes Campus, Mawson Lakes,
SA5095, AUSTRALIA
{matthew.simon, jill.slay}@unisa.edu.au

Abstract. Training, certification and accreditation are concepts that are used in almost all aspects of professional life. This paper reviews current initiatives in Forensic Computing training and certification in Australia and the effect of this on National Accreditation processes.

Keywords: Forensic Computing; Training; Certification; Education.

1 Introduction

Training, certification and accreditation are concepts that are used in almost all aspects of professional life. The level of training required for most jobs can vary substantially from zero, to on the job training, to a degree qualification. Driving a forklift in South Australia requires the operator to hold a forklift licence. To get a licence, the applicant must be "*assessed by a registered assessor as being competent to operate the equipment in accordance with the competency standards in the national loadshifting guidelines*" [1]. In this case, the licence certifies that the holder can operate a forklift to an acceptable standard. Similarly, a medical doctor may need to study for up to seven years, and then do an internship before getting a medical licence. Certification shows that the certified entity meets specific competencies or criteria [2] . It not only allows people to make judgements based on that certification, but also provides a constant minimum standard.

Within the field of forensic computing there is currently a problem with both training and certification of practitioners, and the accreditation of laboratories. This is because there is no unified list of standards and competencies within the domain [3]. The domain is not without some certifications and accreditations, for example, ISO 17025 can be applied to accredit any general laboratory and ASCLD-LAB is a special purpose forensic laboratory accreditation. These accreditations have had a positive impact on the direction of the development of the forensic computing field. Beckett [2] references prominent authors in the field of forensic computing who have commented on the "*chaotic*" manner in which the field has developed in the ten years previous,

Please use the following format when citing this chapter:

Simon, M., Slay, J., 2007, in IFIP International Federation for Information Processing, Volume 237, Fifth World Conference on Information Security Education, eds. Futcher, L., Dodge, R., (Boston: Springer), pp. 105–112.

attributing this mainly to a lack of formal and standardised certification. This development of the field has prevented forensic computing from being regarded as a mature forensic science.

2 Background

Forensic computing can be described as the investigation into criminal or unethical activities which may have left digital evidence (Mohay 2005). Although this definition appears simplistic, it specifies the existence of digital evidence, which is the very core of *'computing'* in the term forensic computing. The *forensic* aspect of forensic computing is equally important and - in a modern sense,- literally describes *"any professional practice that provides scientific knowledge to the trier of fact"* [2] . Beckett [2] lists a number of disciplines which have common forensic applications such as Biology, Firearms-Ballistics and Handwriting. Patel and Ó Ciardhuáin [4] describe the purpose of forensic computing as *"...to collect tangible evidence showing that some unacceptable action has been carried out using methods which are themselves acceptable"*. Defining acceptable methods for use within forensic computing is problematic due to a lack of standardised certification, accreditation and training within the field.

The forensic practices and processes used to recover and evaluate evidence during an investigation are of the utmost importance as it is likely they will be scrutinised when presented in court. Having a sound investigation technique is crucial for evidence admissibility and credibility of the investigators. The issue currently facing forensic computing is a lack of consistent standards and competencies to unify the field as a solid science [2]. Compared with other domains of forensic science - some of which are over 100 years old - forensic computing is relatively young and is still developing. These other fields have had time to mature and as such have developed formal methodologies, standards and competencies.

It is generally accepted that a professional career in most domains is based on a specific body of knowledge, training and accreditation. However, this does not appear to be the case in forensic computing. Valli (cited in [2]) points out that information technology commonly relies on certification rather than formal tertiary qualifications as a means of industry credentials. Beckett [2] further explains by arguing that information technology is the only industry that relies so heavily on such certifications. He goes on to list examples of trade careers which all require a set number of years as an apprentice and formal studies before being fully qualified.

Within Australian Commonwealth law there is no formal specification of what constitutes an expert witness. It is unclear whether an expert must have relevant formal qualifications or if experience alone is enough [5]. A person who has completed a vendor-based course –an EnCase user course for example- may claim to be an expert witness simply because they can use and understand output from the specific tool. Beckett [2] however, contends that an expert should have greater knowledge than how to use a single tool as a greater understanding of the material being examined is required. Meyers & Rogers [3] report that no evidence has yet been made inadmissible as a direct result of not knowing the internal workings of the software, but this does

not mean that it is not a future possibility. McDougall [6] lists guidelines specified by the New South Wales Supreme Court for allowing expert testimony:

1. it must be agreed or demonstrated that there is a field of "specialised knowledge";
2. there must be an identified aspect of that field in which the witness demonstrates that by reason of specified training, study or experience, the witness has become an expert;
3. the opinion proffered must be "wholly or substantially based on the witness's expert knowledge";
4. so far as the opinion is based on facts "observed" by the expert, they must be identified and admissibly proved by the expert;
5. so far as the opinion is based on "assumed" or "accepted" facts, they must be identified and proved in some other way;
6. it must be established that the facts on which the opinion is based form a proper foundation for it; and the expert's evidence must explain how the field of "specialised knowledge" in which the witness is expert, and on which the opinion is "wholly or substantially based" applies to the facts assumed or observed so as to produce the opinion propounded.

From the criteria above, doubt could raised as to the admissibility of expert opinion from a (solely) vendor certified practitioner. Criteria two is in doubt as it is questionable whether being an expert at using a tool is considered an expert in the field. Criteria six also raises doubt as "the expert's evidence must explain how the field of 'specialised knowledge'... applies to the facts assumed or observed so as to produce the opinion propounded". It is unlikely that such an expert could formulate and justify opinions with such narrow and specific training. It is imperative that standards and certifications be established in forensic computing for the purpose of identifying qualified expert witnesses [7]

3 Available Certifications and Accreditations

Training, certification and accreditation in computer forensics is varied in nature and quality. The difference between certification and accreditation is to whom or to what it applies. Both confirm a certain level of competence in meeting a given set of criteria. Certification applies to an individual such as a computer forensic analyst whereas accreditation applies to an organisation - in this case it will most likely be a forensic laboratory. An accredited computer forensic laboratory guarantees acceptable facilities, a defined process model, appropriately trained, educated and qualified practitioners, and quality assurance measures[8]. Certified practitioners on the other hand, are guaranteed to have a minimum set of KSA's (Knowledge, Skills, and Abilities) that vary depending on the particular certification in that is held.

3.1 Certification in Forensic Computing

The Certified Computer Examiner (CCE) certification is overseen by an organisation called the International Society of Forensic Computer Examiners (ISFCE) (http://www.isfce.com/). ISFCE is a private, for profit organisation and has strict requirements for holders of the certification. There are no prerequisites for attending the course although there is a level of expected knowledge. A multiple-choice test is available online, which can be taken at no cost, designed to test if the applicant has the required knowledge to sit for the course. Some of the more difficult questions in the online test are: (Key Computer Service 2006b)
"While at a DOS or command prompt, how would you delete a file called FILE1?"
"Have you ever connected/disconnected the keyboard, mouse or monitor on a computer?"
"Are the keyboard and monitor connectors the same on a standard PC?"

The level of knowledge required to answer these questions is relatively low and it is likely that the average middle school student could answer these successfully. The course page indicates that the necessary knowledge to become an expert witness is taught in the course[9]. It is questionable whether it is possible to become an expert just by completing a five-day course. There are other certifications available that are of a similar standard. GIAC Certified Forensics Analyst (GCFA) (http://www.giac.org/certifications/security/gcfa.php) involves a five day training course and a test for the approximate cost of $3200.00 (USD); no prior investigation experience or training is necessary.
A brief investigation into certification in more traditional branches of forensics shows a considerably different approach. The International Association for Identification (IAI) (http://www.theiai.org) offers numerous certifications. The 'Bloodstain Pattern Examiner Certification' is one such certification. The first requirement is 40 hours of education in approved workshops. This requirement can be fulfilled in a five-day period, equalling the whole CCE certification course training time. Further to the 40 hours, to obtain the 'Bloodstain Pattern Examiner Certification' the applicant must also have at least three years experience in the field of bloodstain pattern identification and a further 200 hours of study. This accreditation is clearly more complex and thorough than the forensic computing equivalent.

3.2 Higher Education

Higher education in Australia offers little in the way of computer forensic education. No degree program, like a Bachelor of Forensic Computing, or some such similar degree exist. A number of universities in Australia do offer courses that can be taken as an elective during a computer science programme. The University of South Australia (http://www.unisa.edu.au) offers a fourth year course called 'Forensic Computing: Tools, Techniques and Investigations'. The course curriculum covers many of the basic areas of computer forensics including investigation, legal issues, crime scene management, data collection from various operating systems and standard forensic com-

puting tools. Central Queensland University (http://www.cqu.edu.au) includes computer forensics in a network security course, but does not go into detail. The University of Western Sydney (http://www.uws.edu.au/) offers one of the more specialist forensic computing courses available in Australia. It offers a traditional Bachelor of Computer Science with a major in forensic computing. To complete the degree with that particular major there are a number of compulsory courses. 'Computer Forensic Workshop', 'Operating Systems', 'System Administration Programming', 'Information Security', 'Network Security' and 'Information Systems, Ethics and Law' are all required to major in forensic computing. The Canberra Institute of Technology (http://www.cit.act.edu.au) offers an advanced diploma course in forensic computing; the only higher education course that focuses purely on forensic computing. The website asserts that the course will qualify the person for a job as an "investigator specialising in electronic data evidence including electronic fraud, computer crime investigators, and data recovery specialists".
Gottschalk & Liu [10] conducted a survey of higher education institutes offering edification in forensic computing in the USA. They found 32 different forensic computing related programmes including eight two-year diploma programmes, four four-year degree programmes, four master courses, three graduate certificate programmes and 13 non-graduate certificate programmes.

3.3 Law Enforcement Only

Law enforcement training programmes are not open for public attendance as applicants must be affiliated with a law enforcement agency i.e. both sworn and non-sworn officers can attend. The International Association of Computer Investigative Specialists (IACIS) (http://www.iacis.info/iacisv2/pages/home.php) is a not-for-profit organisation in which membership is only open to law enforcement. The agency offers a variety of courses on different topics and at varying lengths. Two-week courses are run annually, called Forensic Training Courses. They allow attendees to obtain grounding in computer forensic. Members attending courses in subsequent years can elect to take more advanced topics rather than the general stream.
Vendor specific software training is often based on a specific tool or set of tools that is run by the company that owns the tools and these are often delivered for Law Enforcement. These courses can be useful in obtaining training in the specific tools but the weaknesses of the tools may not be made evident [11].

3.5 Accreditations

Within the computer forensic discipline very few accreditations are available than can be used for a forensic computing laboratory. There are three main accreditations commonly used in the field including the 'American Society for Crime Laboratory Directors/Laboratory Accreditation Board' (ASCLD/LAB), the National Association of Testing Authorities (NATA) and ISO 17025 (General Requirements for the Competence of Testing and Calibration Laboratories) [2]. ISO 17025 is not specifically a

computer forensic laboratory accreditation (or even a general forensic laboratory accreditation) but rather aimed at any laboratory which is involved in testing or calibration. ISO 17025 verifies that laboratories measurement and decisions are accurate, repeatable, believable and verifiable, delivered in a timely manner and all opinions and recommendations are based on a proper process.

The ASCLD/LAB has two different accreditation programmes, ASCLD/LAB-Legacy and ASCLD/LAB-International. The ASCLD/LAB-Legacy accreditation was developed in 1982 but did not formally recognise forensic computing until July 2003 (Barbara 2004). The ASCLD/LAB-International accreditation is an extension of the ISO 17025 standard. The requirements in addition to ISO 17025 are important parts of the Legacy accreditation not covered under ISO 17025 (Barbara 2004; American Society of Crime Laboratory Directors 2006). As of 16 September 2006, there were 317 laboratories accredited under one of the two ASCLD/LAB accreditations, 204 under Legacy and 13 under the International program. Of the 13 ASCLD/LAB-International accredited laboratories, only one is a digital evidence laboratory [12].

The NATA is an Australian based laboratory accreditation that is similar to the ASCLD-International accreditation as it is implemented on top of ISO 17025. It is recorded as being the oldest certification of that type in the world [13]. Unlike the ASCLD accreditations, NATA is used to recognise any type of testing and calibration laboratory, not just forensic orientated facilities. The NATA website lists 35095 laboratories which have achieved accreditation; only 23 of these are information technology facilities, and none of these are digital evidence based (NATA 2006a). At least one forensic computing laboratory in Australia is currently working towards obtaining the standard [14].

It is important to note that individual examiners working within the accredited laboratory are not certified under any of the accreditation mentioned. Examiners do, however, need to be certified and this is commonly done by the accredited organisation using an internal certification programme [15].

4 Discussion and Conclusion

Forensic Computing is making progress towards becoming a solid forensic science. A number of factors have delayed the transition from the unsystematic computer forensics of the past to the modern structure of the field. Although progress is being made, there is still much development to occur before the industry can be regarded in the same way as traditional forensic disciplines like forensic accounting or forensic ballistics. The major problem that has been plaguing the discipline of forensic computing is the lack of standards and formal methodologies. This can largely be attributed to the relative immaturity of the field and has lead to deficiencies in the quality of training, certification and accreditation of practitioners and laboratories within the field. By comparing the available options for training, certification and accreditation to those of traditional branches of forensic science, it is clear that the forensic computing domain is still missing essential elements of cohesion and authority.

The initial lack of standards and formal methodologies has created a problematic environment. Numerous third party and vendor based training and certifications are of-

fered that are aimed at training forensic practitioners to fulfill the market demand caused by those joining the field. This in turn has stunted the development of formal KSA's (Knowledge, Skills and Abilities) for practitioners and methodologies within the field in general. An additional problem with the certification-based model is inequality of those claiming to be experts, and furthermore, those claiming to be qualified to give expert testimony in a court of law. The very definition of an expert must be clarified by an accepted industry standard in order to begin to rectify the problem. Forensic 'experts' are currently testifying in courts and providing opinion evidence that is taken into account by the 'trier of fact'. There must be justification of the ability of the person to provide such evidence in order to maintain an acceptable legal standard.

The problem goes further than just the abilities of the individual forensic practitioner. Digital forensic laboratory accreditation has only recently become available and this is having a positive impact on the maturity of the field. Beckett [14] argues: "the push to validate the filed as a true forensic science is now being driven by these accreditation standards rather than allow the field to develop in the chaotic manner that has been observed over the last decade". Stringent standards must be implemented and maintained in order to obtain and keep such accreditations. This is instrumental in developing a high level of confidence in output from such laboratories.

The development of laboratory standards has recently started to raise the credibility of forensic computing, but there is still progress to be made for training and certification of individual practitioners. There are a variety of different training programmes available and several individual certifications that can be obtained, but no national or international standard proficiency testing currently exists. A lack of such a testing protocol results in no formal method of defining different levels of practitioners and no way to verify a person who claims to be an expert. All other forensic disciplines have formal methodologies, KSA's, national or international bodies to oversee to field and require minimum standards of tertiary education to practice in the field. Digital Forensics is now developing in a positive direction, encouraged by vendor neutral and internationally recognised accreditations for digital evidence laboratories. Certification in digital forensics needs to be replaced with formal tertiary qualifications and proficiency reviews to determine that all practitioners meet minimum KSA's. Certification is likely to continue to play a role within the domain and verify additional skills. A qualified practitioner may obtain a certification as a 'certified EnCase user' that shows knowledge of the tool rather than knowledge of the field as is the current state. Future development in this direction will see digital forensics unequivocally move into the modern age and become a solid and respected science.

References

1. Occupational Health, Safety and Welfare Regulations (SA) 1986.
2. Beckett, J 2006, Personal communication.
3. Meyers, M & Rogers, M 2004, 'Computer Forensics: The Need for Standardization and Certification', International Journal of Digital Evidence, vol. 3, no. 2.

4. Patel, A & Ó Ciardhuáin, S 2000, 'The impact of forensic computing on telecommunications', IEEE Communications Magazine, vol. 38, no. 11, November 2000, pp. 64-67.
5. Australian Law Reform Commission 1985, Opinion Evidence, viewed October 2006, <http://138.25.65.50/au/other/alrc/publications/reports/26/Ch_14.html>.
6. McDougall, R 2006, Exp ert Evidence, updated 5 March 2006, Supreme Court, NSW, viewed 17 September 2006, <http://www.lawlink.nsw.gov.au/lawlink/Supreme_Court/ll_sc.nsf/pages/SCO_mcdougall130204>.
7. G.Shpantzer & T.Ipsen 2002, 'Law Enforcement Challenges in Digital Forensics', paper presented at the Colloquium on Information Systems Security Education.
8. Pollit, MM 2005, Digital Forensic Accreditation, Certification and Standards, National Center for Forensic Science, viewed 22 September 2006, <www.ncfs.org/dcfb/DFCB101205.ppt>.
9. Key Computer Service 2006b, Thank you for your interest in our training, viewed 20 September 2006, <http://www.cce-bootcamp.com/pretest.htm>.
10. Gottschalk, L & Liu, J 2005, 'Computer Forensics Programs in Higher Education: A Preliminary Study', paper presented at the Technical Symposium on Computer Science Education, St Louis, Missouri, USA, Feb 23-27.
11. Kuchta, KJ 2001, 'Learning the Computer Forensic Way', Information Systems Security, vol. 10, no. 5.
12. American Society of Crime Laboratory Directors 2006, Laboratories Accredited by ASCLD/LAB, updated 16 September, 2006, viewed 22 September 2006, <http://www.ascld-lab.org.legacy/aslablegacylabdirectories.html>.
13. NATA 2006, The History of the National Association of Testing Authorities, Australia, viewed September 22 2006, <www.nata.asn.au/index.cfm?objectid=1D70401C-FB17-96FC-3860E377EF629C43>
14. Beckett, J 2005, 'Forensic Computing Experts, Certification and Categorisation of Roles', paper presented at the Colloquium for the Information Systems Security Education - Asia Pacific, Adelaide, Australia.
15. Barbara, JJ 2004, Digital Evidence Accreditation, viewed 22 September 2006, <http://www.forensicmag.com/articles.asp?pid=28>.