2006

Establishing a vendor neutral skills based framework for digital forensics curriculum development and competence assessment

Craig Valli
Edith Cowan University

Establishing a vendor neutral skills based framework for digital forensics curriculum development and competence assessment

Craig Valli
Edith Cowan University
c.valli@ecu.edu.au

Abstract

This paper outlines an approach being undertaken between ECU and the Australian Electronic Evidence Special Advisory Group (EESAG) in the production of vendor neutral skills matrix for developing curriculum and evaluating competence. The framework is constructed using Blooms Taxonomy of Learning. This is a work in progress paper and covers the inital stages of the development

Keywords competency, forensics, learning, framework, vendor, evidence, curriculum

INTRODUCTION

One of the challenges for computer science educators in recent years is the encroachment of the computer science space by vendor based training masquerading as education. The area of computer or digital forensics is also suffering from glib advertising by trainers and vendors stating such things as become a computer forensics expert in 24 hours or five-day computer forensics boot camp. Furthermore vendor specific training is little more than a certification program for a particular product even if it is "industry standard"(Valli, 2003). Just because someone can use a technology does not mean that they are suitably credentialed and have an expert understanding of it from first principles a good example of this is a modern automobile. While there is nothing wrong with this as an approach to training it often does little to develop the overall skill and competence of a forensic examiner due to its narrow product specific focused curriculum. Furthermore, while essential that one can demonstration proficiency by possibly gaining the industry certification it does little to assess competence as an expert beyond use of the package/system.

Expertise in digital forensics requires a wide range of expertise within the computer science discipline from basic concepts such as number systems and arithmetic through to complex skills in process and concepts involved for instance in the acquisition of a live RAID disk subsystem. This level of complexity cannot be demonstrated nor tested using a multiple choice test. Assessment of skills in this discipline should involve witnessing of both the theoretical aspects and practical execution of skills to achieve a particular process or outcome.

This paper outlines an approach being undertaken between Edith Cowan University and Electronic Evidence Special Advisory Group in the production of vendor neutral skills matrix for developing curriculum and also for evaluating competence of electronic evidence or digital forensic examiners.

THE NEED FOR A FRAMEWORK

Currently there exists little in the way of cogent educationally based frameworks or curriculum for digital forensics. Although the discipline is a relative newcomer in the computer science area many of the principles of operation and theory underpinnings are the same as existing subject material within computer science praxis.

One of the other dangers of the current status quo within the digital forensics domain is that a lot of the "education" is vendor driven training. This form of "education" being offered is in reality specific training about a vendor's product and execution of same to achieve forensics outcomes with that given product. This is not education it is training and as such should be sold as that. Education is about theories and principles of operation to enable lifelong learning whereas training is atypically lock step instruction to achieve an end goal with a given tool. To illustrate the point further, take the case of Person A was trained in a particular computer language or they can be educated about the constructs and theories behind programming using that language as a vehicle in this case Person B. When a transition or change is needed to another programming language then Person A will have to be retrained often at considerable expense. Furthermore, by developing skills on a vendor centric approach a professional will tend to see solutions to a problem that may also not be the most expedient or efficient and will end up being tools centric rather than problem or skills centric.

Many previous attempts at creating frameworks have been technology centric which is not ideal for construction of a framework in an area that is rapidly evolving. This is particular problem in the computer industry due to the

high rate of technological obsolescence and also vaporising vendors. Forensics is based in a scientific tradition and adoption of almost a monotheist approach to vendors and solutions is almost the anti-thesis of good science.

For example, the "professional" will become aligned with a particular solution or process which will inevitably not be the best outcome or solution for every case. By being vendor bound also examiners may be less inclined to try alternate avenues of investigation for a particular case the end result of which could be a loss of critical evidence or breakthrough. Furthermore, aligning a framework with a particular vendor in an area that is fluxing to level of digital forensics practise is tenuous. As processes evolve in a science, paragons are re-examined and re-aligned to better fit changing knowledge landscapes and avenues of enquiry.

PRINCIPLES UNDERLYING THE FRAMEWORK

There are two overarching principles for the framework and these are firstly that the framework be vendor neutral and skills centric and second that the framework employ sound educational theories and practise in the development of the framework.

Educational learning theories aid in structuring learning targets and outcomes and are valuable tool in construction of a skills matrix with competency or learning. Most skills are learnt through example, via training or education, very few are innate or intrinsic to a person the concept of tabula rasa. Even the simple ability to dodge a flying object such as a fast moving cricket ball is a too often painfully learned behaviour. One of the major educational frameworks used to construct curricula is Blooms Taxonomy of Learning it is a well established learning taxonomy for the construction of learning artefacts and objects (Bloom, 1984). Blooms Taxonomy consists of six levels of abstraction for categorising skills and knowledge and developing appropriate evaluation mechanisms of same. The levels are Knowledge, Comprehension, Application, Analysis, Synthesis and Evaluation.

THE PROPOSED FRAMEWORK

There will be six levels of expertise rating the level of skill numbered Level 1 through 6. The levels are intended to demonstrate a progressive hierarchy of skill or achievement of process execution ability. These levels are then used to generate activities or performance criteria for attaining certification of a core competency at a particular level. The use of the six levels borrows heavily from Blooms Taxonomy of Learning that elucidates a progression of knowledge and skills acquisition as a progression. The six levels presented in this framework are scaffolded such that each level provides requisite skills for progression and use in the further levels. Progression or certification to a Level is only as a result of achieving mastery of prior levels of expertise. These levels are intended to be discrete and robustly fecund, it is expected that even highly knowledgeable and experienced persons would only achieve Level 6 competency across some domains within the final framework. The levels are outlined below with Blooms levels in brackets:

Level 1 – Define (Knowledge)

This level indicates the lowest level of competency. A person would be able to define what an activity, process or concept is for example

- Define a forensic image
- Define a cryptographic hash

Level 2 – Apply (Comprehension)

This level is indicated by the ability to apply an activity, process or concept.

- Apply a cryptographic hash
- Apply procedure to attain a acquisition of a forensic image

Level 3 – Explain (Application)

This level is indicated by the ability to apply an activity, and explain the process or concept/s.

- Explain how a cryptographic hash is created
- Explain how a forensic image is acquired

Level 4 – Evaluate (Analysis)

This level is indicated by the ability to critically evaluate, analyse an activity, process or concept.

- Evaluate cryptographic hashes for suitability to task
- Evaluate various methods of forensic image acquisition for a given scenario

Level 5 – Critique (Synthesis)

This level is indicated by the ability to critique an activity, process or concept using sound scientific process.

- Critique a use of cryptographic hashes by another examiner. Using a variety of methods to evaluate.
- Critique another examiners acquisition procedure using appropriate methods.

Level 6 – Synthesis (Evaluation)

This level is indicated by the ability to synthesise relevant material to produce an expert report or a validated solution for an activity, process or forensic concept using sound scientific process.

- Produce a expert report on another examiners hard disk acquisition procedure
- Produce a expert report for court on the MD5 hash collision issue
- Solve a multi-partite forensic issue such as acquisition and verification of a live RAID system

The reason for changing the naming conventions is that reducing confusion with standard terms used within the community of practice. An example of this being Analysis being functionality different in Blooms Taxonomy to that of analysis in forensic investigations.

GENERIC CORE COMPETENCIES

There are a set of generic core competencies that are associated with most professions and these are atypically unique and discrete. These core competencies are often the pivotal points of arbitrage and demarcation within, between and among the discipline area. Therefore, logically it should follow that a digital forensic examiner would possess a set of core competencies that are generic to the discipline of digital forensics. These competencies should be linked inextricably to duties or tasks that a forensic examiner must perform in execution of their professional duties. These core competencies should be viewed at the rudiments or skeleton upon which all competence within the area of digital forensics is built upon. The authors posit that the abilities or skills that a digital forensics examiner requires break down into three broad areas of application and competence. These are

Evidence Acquisition

The acquisition and preservation of the original evidence either in-situ or in-stream. This should be down in a sound forensic manner using appropriate tools and techniques with minimal or no modification of original evidence.

Evidence Analysis

The production of scientifically replicable analysis of evidence using sound forensic processes and techniques, using validated, as well as verified technology.

Evidence Report and Presentation

The cogent, lucid, non-polemic presentation and reporting of electronic evidence to external third parties and courts of law.

As an example in this paper we will provide a breakdown of one stream of the framework based upon the Evidence Acquisition as the core competence. The work presented is by no means completed and is illustrative only.

EVIDENCE ACQUISITION SKILLS OUTCOMES AND ASSESSMENT

Outcomes are the end goal or skill base that a digital forensics examiner should aspire to attain to demonstrate competence at a particular level. The following are some possible outcomes for an examiner to have which relate to the acquisition of digital evidence.

It is expected that a competent digital forensic examiner should be able to;

1. Acquire an exact or best possible copy of digital evidence from a digital device or appliance with minimal disturbance of original evidence

2. Explain fundamental principles of computer and forensic science as they apply to the acquisition of digital evidence,
3. Apply valid forensic processes and principles to acquire digital evidence,
4. Validate forensic acquisition processes and outcomes using sound scientific methods,
5. Validate forensic acquisition technology using sound scientific methods and principles,
6. Cogently communicate either verbally or in a written report a process or technique related to acquisition of digital/electronic evidence.

From the outcomes the generation of skill levels or target behaviours can be generated the authors in this paper will explicate some detail for Evidence Acquisition at Outcome 1 at Skill Level 1, 2 and 3. Again the lists of competencies are not complete and are meant as an example only.

Outcome A-1

Acquire an exact or best possible forensic image of a digital device or appliance with minimal or no disturbance of original evidence

Level 1

This level is demonstrated when a candidate can

1. Define forensic image or bit level copy

2. Define a simple procedure to acquire a forensic image of a computer hard disk or USB memory stick using a suitable forensic imaging software

3. Define a cryptographic hash

Level 2

This level is demonstrated when a candidate can

1. Apply a simple procedure to acquire a verified forensic image

2. Apply a cryptographic hash to verify an file, directory or image

Level 3

This level is demonstrated when a candidate can

1. Explain how a cryptographic hash is created and then is able to be used to verify a forensic copy

2. Explain a procedure to acquire a forensic image from a digital device.

3. Explain the concept of a partition and how it relates to an image of magnetic media device.

ASSESSING COMPETENCE/KNOWLEDGE

One of the key elements of the framework is structuring assessment of the skills and knowledge in the framework. Assessment should be able to be achieved via various methods and type to demonstrate proficiency and also provide some triangulation of measure. Furthermore, certain assessment types are better suited to different levels of the framework. It can be argued that multiple choice questions could be used to assess competency at all six levels of the framework. However, these would be complex to construct and possibly not give a candidate an ability to demonstrate competence. Likewise the incorrect use of essay could be a problem for example, a essay question to define what an MD5 Hash is would be inappropriately aligned.

In addition to alignment, the effect of assessment on student learning also needs to be considered. There can be little argument that assessment drives student learning (Ramsden 1992; Weimer 2002; Biggs 2003; Mackinnon and Manathunga 2003). If we wish to get students to learn, there are two critical aims which must be addressed. Firstly, the content and teaching practices must match the course objectives, and secondly, the assessment must align with the outcomes expected and be relevant to the level of understanding required for that subject. Objectives requiring higher level engagement must be assessed using appropriate assessment techniques. In relation to competencies for digital investigators,

Feedback is an essential tool if students are to learn through assessment. Ramsden (1992) states that a lack of feedback not only causes angst in the students, but is also an attributable cause of failure in first year students.

The following table gives indicative methods of assessment matched against the proposed framework that could be used within the digital forensics paradigm to achieve

Level		Suitable Assessment Type
1	**Define**	Multiple Choice Test Written Test – Short Answer
2	**Apply**	Practical Test
3	**Explain**	Practical Test Written Test – Essay, Short Answer
4	**Evaluate**	Written Test – Essay, Short Answer Case Analysis
5	**Critique**	Written Test – Essay Case Analysis/Defence
6	**Synthesis**	Written Test – Essay Practical Test Case Analysis/Defence

Table 1 – Suitable Assessment Types

To demonstrate competence in Level 1 atypically requires rote learning of basic facts relating to the relevant outcome. Mastery of this level is adequately demonstrated by using multiple choice or short answer as outlined in Table 1 as the primary assessment mechanism.

Level 2 is the application of rudimentary concepts and processes learned from Level 1 attainment. Demonstration of mastery at this level is best assessed by practical application of the concept/process under test conditions. In the example above one of the Level 2 outcomes indicators was *Apply a simple procedure to acquire a verified forensic image.*

To test this skill a person could be practically tested in their ability to apply a given procedure to the acquisition and verification of a forensic image. The actual procedure could be of the candidates instantiation or be based on a departmental or standard process used by the validating organisation. It is critical that the acquisition and verification of the forensic image are closely observed and assessed in the evaluation process.

Level 3 is again progressing from previous levels the candidate must now combine and use their knowledge of the area demonstrating the ability to explain a concept or process. It is envisaged that this stage represents the basic level of competence for a digital forensic examiner that would be capable of presenting material to court, tribunal or third party.

In the example above *Explain a procedure to acquire a forensic image from a digital device* would mean that an examiner could explain the underpinning concepts, processes and procedures required to acquire a forensic image. Assessment of this skill can be undertaken in a written test or peer evaluation of the elocution of the candidate upon the subject matter. Practical demonstration with dialogue and instruction would also demonstrate mastery at this level.

Assessment is a difficult subject and it is not the aim of this paper to provide an overly academic exploration of this at this point in time. However, once the initial framework is developed an empirical learning approach will be taken towards production of assessment artefacts. It also envisaged that some form of validation and audit process will be undertaken to ensure that assessment is applied consistently to ensure quality.

FUTURE WORK

Currently work on the framework is limited to expanding the first three levels of the framework as it is felt that this is the rudimentary level of skill or competence that a digital forensic examiner requires to function in the vocation. The framework is designed to be vendor neutral and also be able to be used in various jurisdictions and communities of practice within the electronic evidence/digital forensics discipline.

One of the major challenges in producing the framework will be the common language or nomenclature used in its construction. To describe the emergent discipline area alone there are computer forensics, forensic

computing, digital forensics or electronic evidence as candidates. Another example the end result of evidence acquisition on secondary memory device such as a hard disk or USB device is it a forensic image or mirror copy that is produced? While the framework in itself directly does not attempt to solve these questions it could be said that as a secondary outcome its purpose is to form a framework from which to articulate argument about the correct terms for use within this discipline area.

Sound educational practise also mandates a variety of delivery models, techniques and assessment practises to ensure that learning and assessment is complete and not subject to challenge. Furthermore, quality control of this assessment must also be inculcated to the point where it becomes intrinsically embedded within the framework. These assessment artefacts and supporting framework will only improve through adoption of a empirical learning approach and a process of review and reflection by all parties involved in the process, grounded in sound theory and praxis.

REFERENCES

Biggs, J. B. (2003). *Teaching for quality learning at university*. Berkshire, Society for Research into Higher Education : Open University Press.

Bloom, B. S. (1984). *Taxonomy of educational objectives*. Boston, MA: Allyn and Bacon by Pearson Education.

Entwistle, N. and D. Entwistle (2003). Preparing for Examinations: The interplay of memorising and understanding, and the development of knowledge objects. *Higher Education Research & Development* **22**(1): 19-41.

MacKinnon, D. & Manathunga, C. (2003). Going global with assessment: What to do when the dominant cultures literacy drives assessment. *Higher Education Research and Development*. **22(2):** 131-144

Ramsden, P. (1992). *Learning to teach in higher education.* London, Routledge

Weimer, M. (2002). *Learner-centred teaching: five key changes to practice*. San Francisco, John Wiley and Sons.

Valli, C. (2003). *Industry Certifications: Challenges For The Conduct Of University Security Based Courses.* Paper presented at the 4th Australian Information Warfare and Security Conference, Adelaide, South Australia.

COPYRIGHT