An Analysis of Computer Forensic Practitioners Perspectives on Education and Training Requirements

Colin J. Armstrong

Gailaad Pty Ltd, Perth,
Western Australia
ColinArmstrong@gailaad.com

Abstract. It could be argued that the academic perspective of computer forensic practitioner requirements reflecting the thinking world (and is based on scientific methods) does not accurately reflect those requirements considered important by some people universities would desire as students, the computer forensic practitioners. This paper presents an analysis of data collected from full time practitioners representing three perspectives; military, law enforcement, and forensic scientist. It also examines the needs of practitioners and compares these with academic contributions intended to meet these needs.

Keywords: Academic education programs, Vendor training courses, practitioner education and training needs.

1 Introduction

Much has been written about the importance of evidence integrity but it is the credibility of the forensic practitioner called as an expert witness that may be crucial to the outcome of a case [1]. The most important tool in any computer forensic practitioner's kitbag is their personal integrity. Once doubt is cast upon a practitioner's personal integrity, it matters little how well they conduct their duties. A court or jury may have sufficient doubt of the practitioner's abilities, impartiality, or intentions as to render a successful prosecution impractical. Undertaking and engaging in training and educational programs form an important aspect of developing the perceived integrity of a forensic practitioner.

Both universities and other training and educational providers have long understood the importance of meeting these needs and offer a multitude of courses designed to facilitate meeting student's desired learning outcomes. At Curtin University, Western Australia, programs have an underlying philosophy that should produce a graduate with a set of essential generic skills intended to help them become a "problem solver" first, and a specialist domain expert second [7]. Teaching computer forensics at Curtin University is intended primarily to meet industry demands where the combination of academic research, teaching and training to support industry and law enforcement should improve confidence and credibility of investigators [2].

Slade [14] reiterates the risk that findings and opinions may be dismissed by a court where a computer forensic expert cannot prove sufficient knowledge, education, skill and experience. Kruse and Heiser [11] state that specialists in the field need to

be flexible and engage in continually learning, and Vatis [15], Littlejohn and Tittel [12], and Warren [16], remind us that by working together, researchers in academia, industry, and government can give our public servants and practitioners the tools skills and knowledge they need to address issues of critical public security. Students however tend to be locked into solution based skills and therefore have difficulty in understanding the 'real' problems of the end-users. Methodologies they learn have solutions and solution notions embedded in them that make it difficult to consider the real nature of problems. Jayaratna [10] defined these as "solution driven opportunities seeking methodologies." Armstrong and Jayaratna [7] also discuss the problem of practitioners finding it difficult to recognize the changes taking place in their own specialist field because they have mastered a set of skills which they are reluctant to sacrifice or to master a new set of skills because of the time investment required.

At the same time those not necessarily concerned with integrity have at their disposal the Internet which holds the capacity to provide the facilities for people with criminal intent to associate and exchange intelligence and acquire skills [4]. Roast, Lavender and Wisniewski [13] state that criminal exploitation of new technologies has brought about three main results: new forms of crime, more traditional forms of crime being committed in new ways that increase benefits or reduce risks to offender, and the more general use of the technologies by offenders, to organise, to communicate, and to shield their activities from surveillance. Eurim [9], reports that the Internet is attractive to criminals because it provides opportunities for stealth and anonymity with the opportunity to automate and organise multiple crimes whilst remaining unseen and possibly undetected.

The problem situation is compounded by the recognition of the perception that exiting solutions are inadequate. Broersma [8] states that the criminal justice system, particularly in the UK, is ill-equipped to handle computer related crime, emphasising that among other challenges, the investigation of crimes require better technical skills. Whilst law enforcement computer forensic practitioners strive to maintain high levels of skill competencies, the majority of police officers are not highly trained in computing and those with a good knowledge of computers or specialist skills in electronic evidence rarely attend the initial investigation at the scene of a crime [5]. This invariably results in vital electronic evidence on computer systems and electronic devices being either overlooked or unwittingly contaminated.

Often computer forensic practitioners have to rely on the police officer in the field to seize and protect the evidence with the attendant risk that a mistake at the scene could cause loss of credibility to the computer forensics investigating officer in any subsequent legal hearing [2].

That academia can provide skills based solutions to law enforcement field offices successfully is discussed by Armstrong and Russo [5]. A significant contributor to the successful outcome of the training project used in preparation to Operation Auxin was that it closely preceded the police operation. Operation Auxin, which resulted in the arrest of approximately 200 people, was the Australian part of the September 2004 US - FBI Operation Falcon, a cooperative international law enforcement operation against organized paedophilia. Detectives and uniformed police faced their in the field ‘practical examination’ when they were forced to apply the knowledge in situ shortly after undertaking training. There was some concern that had the period between the training and practical application been longer the success of the operation

may not have been so high. Feedback from the operation participants reinforced the opinion that the constantly changing nature of equipment and media containing potential electronic evidence makes the need for frequent updated training essential [5].

Eurim [9] together with the UK Institute for Public Policy Research (IPPR) recommend greater training opportunities for police in e-crime and computer forensics stating "New skills are required at all levels within the police and supporting services to enable investigators and forensics experts to trace and analyse criminal activities that involve computers and networks and to gather intelligence from them. New and different techniques are needed to ensure the provenance of evidence in digital form" [9].

2 The Challenge

This then is the problem situation, law enforcement in general and practitioners in particular face both rapidly evolving scientific technology together with a rapidly changing and opportunistic criminal, whilst being required to maintain high levels of competency and enduring a reluctance to abandon mastered skills in order to attain new replacement skills. It is into this mix that both academia and vendors attempt to provide ideal solutions. Because sufficient international data has not been collected and analysed, it is not practical to accurately know all practitioner requirements leading both academia and vendors to provide only the best they can. This paper offers an insight into the practitioner requirements based on data collected from a variety of computer forensic practitioners. None of the practitioners participating in this Survey were students at Curtin University, and of those engaged in university studies were undertaken on a part time basis whilst in full time employment.

3 Practitioner Survey Results and Analysis

Data discussed and presented in this paper is drawn as a subset from a larger survey. Data was collected from practitioner respondents by means of an individually recorded semi-structured interview process [3]. All participants practiced in Australia with the exception of one USA based forensic scientist. Only practitioners employed in a full time capacity were included in the Survey. The three perspectives; military, law enforcement, and forensic scientist, of collected practitioner respondents data is represented in Figure 1.

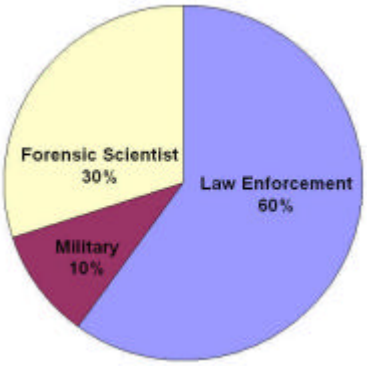

Fig. 1. Respondent Practitioners

The validity of practitioner respondent's entitlement to participate and provide data in the interview process is justified by their responses to the questions shown in Figure 2. Figures 3 and 4 depict years of experience and number of cases worked.

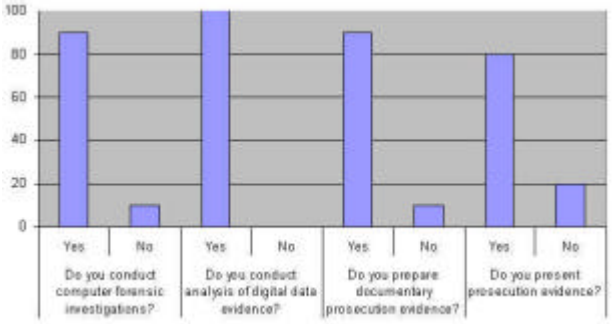

Fig. 2. Clarification of Respondent Practitioner Roles

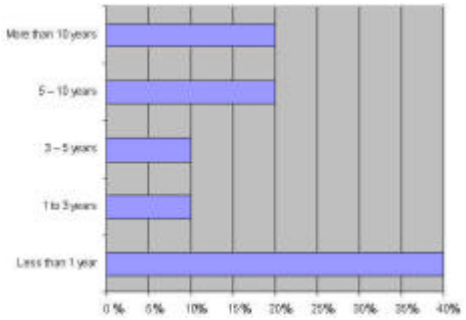

Fig. 3. Respondent Practitioners Experience: Years

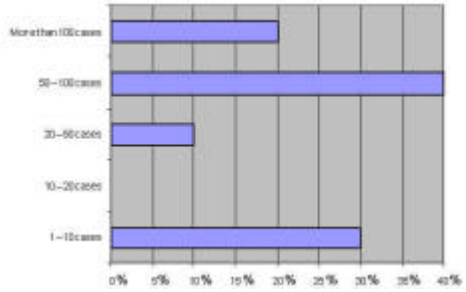

Fig. 4. Respondent Practitioners Experience: Cases

While Figures 1 2 3 and 4 provide an indication of respondent practitioner's proficiency, it is not practicable to estimate an individual's level of competency. All of the practitioners interviewed expressed the opinion that it is desirable that there be a system by which they may determine their personal level of competence [3]. Such a system could permit a practitioner to support a claim of their competency when being assessed by peers, superiors and the Court. While such a system need not be complex it should both provide a uniform or consistent measure whereby they can demonstrate their proficiency and advancement of their skills over a period of time and be internationally recognised, but that discussion is a matter for another paper. This paper focuses on the responses collected from respondent practitioners pertaining to their expressed opinions relating to their previous and desired future training and education which was but one section of the multi-section survey undertaken.

The section of the survey relating to vendor training consisted of a number of questions, the first being: "What short training or educational courses have you undertaken that directly relates to computer forensic and digital data evidence analysis?"

Table 1. Short Training Courses Attended in Order of Popularity.

1	SMART - Advanced
2	FTK Advanced
3	FTK Intro
4	Encase Intro
5	White Wolf Haking 101 / 102
6	Compumatics Cert. Comp Engineer – RS101
7	SMART - Intro & Advanced
8	RedHat RHCT
9	Encase Intermediate
10	Encase Intermediate & Advanced
11	EnCase – Intro & Intermediate
12	SMART - Intro
13	ITAC Applied Hacking
14	Ernst & Young: Extreme Hacking
15	Advanced NTFS
16	Beta release of an in house tool Training Course

100% of respondent practitioners attended multiple short training courses specifically identifying 16 of these. These short training courses ranged in duration from 3

to 20 days with 5 days being the norm with an average duration of 9.6 days. The short training courses undertaken are presented by order of popularity in Table 1 showing the course attended by the most practitioners as being the most popular.

Question 2 asked, "What other training or educational courses have you undertaken that you believe assists you in computer forensic and digital data evidence analysis?" Again, 100% of respondent practitioners attended additional education or training courses identifying three types of programs;

(a.) University (Bachelor, Masters Degrees & Graduate Certificates, plus technical education certificates in Interactive Multimedia),

(b.) Police (Diploma of Criminal Investigation at the Police Academy, General Investigators Course, Specialist Courses and Detective School), and

(c.) Industry Courses (Microsoft Cert Sys Engineer, A+ Hands On & Computer Professional, Compumatics Cert. Comp Engineer – RS101).

Respondent practitioners on average had attended 3 additional educational programs which ranged in duration from 30 days to 3 years equivalent full time study with an average duration being of greater than 1 year equivalent full time study. The educational programs undertaken are presented by order of popularity in Table 2. showing the programs attended by the most practitioners as being the most popular.

Table 2. Educational Programs Attended in Order of Popularity.

1	Police Academy Programs
2	Bachelor Science (Computer Science)
3	Master Science (Computer Security)
4	Graduate Diploma (Computer Science)
5	Graduate Certificate: Information Security
6	Microsoft Certified Systems Engineer
7	A+ Programs

Question 3 asked, "How have these training and educational programs assisted you in computer forensic and digital data evidence analysis?" Respondent practitioners identified a few similar core benefits that each expressed differently and may be categorized into three areas; Knowledge = 50%, Skills = 30% and Leadership = 20%.

The final question in this section asked, "Given the opportunity, what training or educational courses would you undertake that directly relate to computer forensic and digital data evidence analysis?"

100% of respondent practitioners stated a desire to continue engagement in life long learning by attending education and training programs specifying only two of the three types of education programs previously identified: (a.) University (Masters Degrees and Graduate Certificates - shorter & more responsive to needs), and (b.) Industry Courses (advanced vendor training programs, file system programs, A+ Programs, IACIA CF Certification & ENCE). The omission of police courses may be because they address general rather than the specific needs of the respondent practitioners. The educational programs in order of popularity were; (1.) Specialist Advanced Forensic Tool Vendor Training, (2.) Advanced Industry recognised Vendor Programs, (3.) Graduate Certificate (Computer Science), and (4.) Master Science (Internet Security). The respondent practitioners identified only two areas as being beneficial; for

future training and education; Knowledge = 15%, with a concerted emphasis on Skills = 85%.

From the answers given to these questions one may concur that;

(a) practitioners have demonstrated their willingness to engage in both education programs and training courses,
(b) university programs are desirable,
(c) respondent practitioners consider skills orientated programs as most desirable.

It would appear that an ideal solution is to integrate academic courses with a strong theory and conceptual base together with the skills to apply these concepts in practice.

4 Conclusions

Based on the analysis of collected data, one may conclude that respondent practitioners have a strong desire to engage in educational and training programs with an emphasis on gaining firstly practical skills and secondly recognition that accompanies academic qualification. This could be construed to suggest practitioners want the best of two worlds. One world providing the best of practical skills combined with the other world providing academic recognition and where the combination of both worlds offers the perception of better personal integrity to the practitioners.

The acquisition of immediate skills without the opportunity for engagement of thought and time for contemplation builds a capacity that is without a solid theory base and only able to address aspects within its immediate skill set before jeopardizing the practitioner's integrity. Addressing skills only is a short term solution to a long term problem. Academia needs to teach concepts and how to apply them rather than focus on the sales of skills and particular products. The respondent practitioners however, hold as primary importance getting the job done successfully. There is evidence that practitioners on occasion engage in tasks or on work which is undertaken on the basis of trial and error, and conferring with fellow practitioners seeking particular advice when necessary because there is little academic support readily available that is of practical value to the given situation. Vendors attempt to provide single forensic workbench tool as an ultimate solution. Academic rigour requires a period of contemplation time not conducive to maintaining education programs with skills required by respondent practitioners to be readily available today. Both universities and vendors have a duty to continue striving to support practitioners by engaging and working together.

References

1. Armstrong, C. J., 2003. *Developing A Framework for Evaluating Computer Forensic Tools*. Australian Institute of Criminology Conference, Canberra ACT, Australia.
2. Armstrong, C. J., 2003, Mastering Computer Forensics, in *Security Education and Critical Infrastructures*, Irvine, Cynthia and Armstrong, Helen, (Ed's), Kluwer Academic Publishers, Boston, pp 151-158
3. Armstrong, C. J., 2005, *Development of a Research Framework for Selecting Computer Forensic Tools*. Masters Thesis, Curtin University of Technology, Perth, Western Australia.
4. Armstrong, H. and Forde, P., 2003, Cyber criminals and their use of the Internet, *Journal of Information Management & Computer Security*, October, Vol. 11, No. 5.
5. Armstrong, H. and Russo, P., 2004, *Electronic Forensics Education Needs of Law Enforcement*. Conference Proceedings of CISSE8 2004, United States Military Academy, West Point, NY June 2004
6. Armstrong, H. and Russo, P., 2005, *Walking the Beat on the path to technology, Developing computer savvy Police*. Conference Proceedings of WISE4 – 4th World Conference on Information Security Education, May 18-20, Moscow, Russia
7. Armstrong, C. and Jayaratna, N., 2004. *Teaching Computer Forensics: Uniting Practice with Intellect*. CISSE8, United States Military Academy, West Point, NY
8. Broersma, M, 2004, *UK Internet Crime Efforts are Criminal says Study*, Computerworld (Sunday, 23 May 2004), Available on-line @ WWW: http://www.computerworld.co.nz/news.nsf/UNID/BB017D2244CD06D3CC256E9A0073384A
9. EURIM, 2004, *Supplying the Skills for Justice*, Available on-line @ WWW: http://www.eurim.org/consult/ecrime/may_04/ECS_DP3_Skills_040505_web.htm
10. Jayaratna, N. 1999, *Understanding and Evaluating Methodologies. NIMSAD : A Systemic Framework*, McGraw-Hill Book Company, Maidenhead.
11. Kruse Warren G. & Heiser Jay G., 2002, *Computer Forensics: Incident Response Essentials*, Addison-Wesley, Boston
12. Littlejohn Shinder Debra, and Tittel Ed, 2002, *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress
13. Roast, S., Lavender, P. and Wisniewski, T., 2001, Global Impacts, Future Challenges and Current Issues in training within the Police Computer Crime Unit, *Proceedings of the Second World Conference on Information Security Education*, July, Western Australia, pp 7-23
14. Slade Robert, 2004, *Software Forensics: Collecting evidence from the scene of a digital crime*, McGraw-Hill
15. Vatis, M. A., 2002. *Law Enforcement Tools and Technologies for Investigating Cyber Attacks. A National Needs Assessment.* Hanover, NH, Institute for Security Technology Studies at Dartmouth College.
16. Warren, M., 2003, Australia's Agenda for E-security Education and Research, in *Security Education and Critical Infrastructures*, Irvine, Cynthia and Armstrong, Helen, (Ed's), Kluwer Academic Publishers, Boston, pp 109-114