ARTICLE:

PROFESSIONALISM IN DIGITAL FORENSICS[1]

WRITTEN BY:
ALASTAIR D. IRONS AND
ANASTASIA KONSTADOPOULOU

This article considers issues regarding professionalism in digital forensics in order to allow the discipline to develop and to ensure the credibility of the discipline from the different perspectives of practitioners, the criminal justice system and the public. There is a need to examine and develop professionalism in digital forensics in order to promote the discipline and maintain the credibility of the discipline. The paper explores the characteristics of a profession using Denning's criteria,[2] and applies these to digital forensics; attempts to determine the position of the discipline in relation to other forensic science areas and in relation to computer science, and seeks to identify professional issues and challenges for digital forensics and links these challenges to legal and ethical considerations. Consideration is also given to issues such as post-traumatic stress disorder.

The issue of the certification of practitioners is raised, and questions regarding who should certify and what they should be certifying are discussed. The certification issues are, of course, related to the position of the discipline, but are also central to the credibility of the discipline and the ability to ensure robust and due process when digital forensics is applied to the criminal justice system and other disciplines. The role universities have in developing the subject of digital forensics is also considered. An initial version of a practitioner framework is introduced. This is the subject of current work being developed and seeks to take forward the issues raise in this paper as the basis for future certification and accreditation of digital forensics practitioners.

Introduction

There is an increase in the number of investigations, both criminal and civil, that make use of digital forensics, in the number of organisations offering computer forensic services, and in the number of digital forensics practitioners. As a result of this development, there is a need to consider professional issues in order to develop a professional framework that will act to provide a degree of assurance in the skills and expertise of digital forensic practitioners.

Denning's criteria of a profession will be used to discuss professionalism in the digital forensics domain,[3] namely that a profession should:

1. Have an enduring and positive effect on society.
2. Include a codified body of principles (conceptual knowledge).
3. Comprise a codified body of practices (embodied knowledge including competence).
4. Consist of standards for competence, ethics and practice.

It is important to examine professionalism in the context of digital forensics in order to consider the expectations of digital forensic professionals; the amount of knowledge and skill digital forensic professionals require; the ability of digital forensic professionals to resolve digital forensic investigations and problems, and the ability of digital forensic professionals to design the tools, techniques and procedures that will enhance digital forensics as a discipline. This article focuses on the investigative digital forensics practitioner.

One of the main challenges in considering professionalism in the context of digital forensics is that digital forensics is a relatively new discipline, certainly when compared to established disciplines in forensic

[1] *An earlier version of this article was published in the Proceedings of the Second European Conference on Computer Network Defence, in conjunction with the First Workshop on Digital Forensics and Incident Analysis, EC2ND, edited by Andrew Blyth and Iain Sutherland (Springer, 2006), 115 – 125.*

[2] *P. Denning, ' The profession of IT: who are we?' Communications of the ACM, Volume 44, No. 2, 2001, 15 – 19.*

[3] *P. Denning, ' The profession of IT: who are we?' Communications of the ACM, Volume 44, No. 2, 2001, 15 – 19.*

science or computer science. There is a question as to whether digital forensics should be part of the general debate on professionalism in computing – recalling that computing is a new discipline in its own right. Digital forensics as a discipline is further complicated by the speed of technological change and the change in the activities of criminals that use computers to commit crimes.

It is suggested that digital forensics professionals should act with honesty and integrity, be accountable for their actions and have appropriate technical competence, which in turn implies that they should have appropriate qualifications and be members of a suitable professional body. It is also suggested in that it is incumbent upon digital forensics professionals to participate in the following professional duties and responsibilities:

1. Promote digital forensics as a discipline, including the promotion of appropriate professional bodies for digital forensics.
2. Participate in continuous personal professional development.
3. Develop tools and techniques that will enhance the discipline, help the legal process and reduce computer crime.
4. Raise awareness of the benefits to business and society afforded by digital forensics.
5. Participate in creating operational processes and procedures to help counter computer misuse and reduce digital crime.

Professionalism in computing

Organisations such as the British Computer Society subscribe to the notion that the creation, development, management, utilisation and maintenance of computer systems is a professional activity in which qualified computing and IT professionals are recognised and respected. There is a perception that through professionalism in computing and IT, the quality of computer and information systems will be improved. There are a number of professional bodies and organisations such as the British Computer Society (BCS), Institution of Engineering and Technology (IET), Institute of Computer Forensics Professionals (ICFP), Association of Digital Evidence (ADE), Council for Registration of Forensic Practitioners CRFP) or the Forensic Science Society (FSS), which potentially have an interest in digital forensics. However, at present such professional bodies do not have the power to award a licence to practice in digital forensics, and therefore are not able to able to prevent unqualified or under qualified people carrying out digital forensics work. More importantly, the professional bodies are not able to prevent people from offering digital forensics services or practising in digital forensics, and are not able to bar people from the profession as a result of unprofessional practice or misconduct.

From a legal point of view, the regulation of expert witnesses in civil matters in England and Wales is governed by Civil Procedure Rule 35[4] (CPR), Practice Direction – Experts and Assessors, and the 'Protocol for the Instruction of Experts to give Evidence in Civil Claims'.[5] CPR 35.3 makes it plain that the expert has a duty to help out the court 'within his expertise' and this duty overrides any obligation to the person from whom he has received instructions or by whom he is paid. The court controls the admission of expert evidence under the provisions of CPR 35.4. The Protocol provides guidance to experts and to those instructing them, and is intended to help interpret the provisions of CPR 35 and the Practice Direction. The profession will be required to adhered to the requirements of the courts, and any professional body will need to ensure its members are made aware of and conform to the requirements of the courts, for both civil and criminal matters.

There is an ethical aspect to professionalism in digital forensics, in that digital forensics practitioners may find themselves in positions where they have to make choices, whether they be technical, procedural or ethical dilemmas, but all could have an effect on particular cases – for example to ignore a particular source of digital evidence or to fail to investigate a potential source of digital evidence fully. There will often be an element of choice in digital forensics investigations that will potentially have an ethical effect on any decisions made. In effect this means that the digital investigator has the choice to decide what evidence to investigate and corroborate and decide on the depth of the analysis in any particular situation. However, it must be remembered that the investigator has a duty to the court, and if they neglect such a duty, they can face the prospect of legal action being taken against them.

In considering the professionalism of digital forensics,

[4] *The rule, without annotations, is available at http://www.dca.gov.uk/civil/procrules_fin/contents/parts/part35.htm.*

[5] *The Practice Direction and Protocol, without annotations, are available at http://www.dca.gov.uk/civil/procrules_fin/contents/practice_directions/pd_part35.htm.*

there is a need to determine which professional body that digital forensics professionals should be members of, whether forensic science or computer science, or to have a professional body focussing solely on digital forensics. Professional bodies need to take into account the cross-disciplinary nature of digital forensics. This is significant, because there is a link between techniques of investigation, computing technologies and jurisprudence. The different models are set out below.

Forensic science

For example, engaging with forensics science organisations such as the Council for Registration of Forensics Practitioners (CRFP). The British Computer Society were consulted on the proposals put forward by CRFP to register digital evidence specialists, and gave support to the proposed link. Linking with the CRFP would have the benefit of being part of an organization with other forensic science practitioners, but would not necessarily take into account the different nature of digital evidence or the rapid and continual changes in computer technology.

Computer science

Working with professional bodies in computing, such as the British Computer Society or Association of Computing Machinery. These professional bodies are beginning to move towards specialist certification; for example, BCS have advised on forensic practice on digital evidence.

A digital forensics body

Rogers has argued that there is a growing common body of knowledge that establishes digital forensics as a unique area of study.[6] If the discipline establishes itself as a unique discipline, then a professional body dedicated to developing codes of practice and ethics for digital forensics practitioners, and involved in accreditation and certification of digital forensics practitioners may be appropriate. The ACPO Guidelines go some way to addressing standards, but do not determine regulations for practice. Other organisations, such as the International Association of Computer Investigative Specialists and the High Technology Crime Investigation Association focus on the standards for investigative digital forensics practitioners, mainly in law enforcement. The Institute for Computer Forensics Practitioners was established in 2004 to create a "new standardisation, education and foundation of principles and practices in digital forensics that would be open to both public and private sector practitioners".[7]

Not only is there a need to consider the identification of the discipline and where it lies, but also the nature of tasks involved in digital forensics. The credibility of digital forensics must take into account a range of factors that directly affect the competence of the practitioner, such as the development of suitable skills; maintaining knowledge of the changes that take place; the changing nature of computer crime; the continuous need to develop new tools and techniques, and the requirements of the legal environment.

Professional issues in digital forensics

Whilst many of the issues that apply to professionalism in computing also apply to professionalism in digital forensics, there are a different set of professional issues and values that arise due to the nature of digital forensics, forensics investigations and the analysis of digital evidence. In simple terms, if a professional approach is not used in digital forensic investigations, then the investigation and the subsequent trial may be compromised. There are specific professional issues in digital forensics including evidential integrity, evidential continuity and legal issues relating to cases across different jurisdictions. As discussed above, practitioners in digital forensics may find themselves in a situation where they have the opportunity to decide on various aspects of the digital evidence that is being investigated or even to alter digital evidence. As a result, practitioners may find themselves subject to temptation to get involved in computer crime themselves, either by undertaking an action that compromises a particular case, or by carrying out similar crimes as a result of increased knowledge of the potential for crime. Hence there is a need for detailed background and security checks on digital forensics practitioners. In addition, there are a number of legal and ethical considerations that ought to be taken into account, which is the subject of current research being undertaken by the authors.

If Denning's criteria of a profession are considered,[8] it can be seen that digital forensics is moving towards a profession in its own right – to this end digital forensics can draw upon principles and practices from both forensic science and computer science as well as initiate and innovate in developing principles and practices

[6] *M. K. Rogers, 'Computer forensics: science or fad', in Security Wire Digest, 2003, Volume 5, No 65. Available at http://www.cerias.purdue.edu/news/view/88.*

[7] *A. Schroader and N. Dudley-Gough, 'The Institute of Computer Forensics Professionals', Digital Investigation, March 2006, Volume 3, No 1, 9 – 10.*

[8] *P. Denning, 'The profession of IT: who are we?' Communications of the ACM, Volume 44, No. 2, 2001, 15 – 19.*

specific to digital forensics. Consider the criteria:

A set of principles for the greater good of society

Computer crime is an increasing threat to society – at individual, corporate and societal levels. One of the aims of digital forensics as a discipline is to address the threat of computer crime both by increasing the probability of a successful prosecution and by acting as a deterrent to prospective computer criminals. As a result, digital forensics will contribute to making society safer.

A codified body of principles (conceptual knowledge)

Digital forensics is developing a core body of knowledge.[9] In its simplest terms digital forensics is, according to Bates, "the scientific examination and analysis of data held on or retrieved from computer storage media for the purposes of presentation in a court of law, together with the study of the legal aspects of computer use and misuse".[10] The development of a shared set of principles will strengthen the discipline of digital forensics and add credence to the discipline.

A codified body of practices (embodied knowledge including competence)

The ACPO Guidelines[11] are an example of guidelines for practice that identify specific methods and expectations for digital forensic investigations in a criminal context. On the other hand, common methods of investigation will, by their nature, be defined at a high level of abstraction, because of the sheer variety of sources from which digital evidence is found.

Standards for competence, ethics and practice

Common standards are required in digital forensics to ensure consistent approaches in obtaining digital evidence; ensuring it is the digital evidence that the investigation is seeking; and analysing the digital evidence once it has been obtained.

In order to manage standards in a profession, the entry to membership of that profession requires extensive formal education, not just practical training or apprenticeship. An interesting aspect of digital forensics is that because of the rise in computer crime and the demand for people to work in digital forensics, people enter the profession without formal education. Everett estimates that up to 20 per cent of practitioners involved in digital forensics activities are not competent or appropriately certified.[12] The Institute of Computer Forensics Professionals (ICFP) are beginning to develop standards for competence and have put together the development of an ethical code of practice focussing on integrity, impartiality, diligence and objectivity.[13] In order for a professional body in digital forensics to be effective, it needs to have the power to register or certify digital forensics practitioners before they are allowed to practice, and also has to have the power to bar from practice when there have been breaches of code or instances of incompetence.

Certification in digital forensics

Attempts have been made to introduce a licence to practice procedures in computing and software engineering, for example in Texas, in order to enhance the standing of the profession,[14] although questions have been raised about the benefits of certifying computing practitioners and software engineers.[15] In respect of digital forensics, it is necessary to establish whether standards can be defined. Jones argues that "there is an absence of standards and competencies in the field of cybercrime"[16] and although the situation has progressed in the last two years, for example the creation of the register of digital forensics practitioners with the CRFP, there is not a unified position in certification and accreditation.

There are a number of certifications available to the digital forensic practitioner, including qualifications primarily aimed at computer security professionals, such as Certified Information Systems Security Professional (CISSP) from (ISC)2[17] – both of which focus on computer security rather than digital forensics. A number of specific digital forensic certifications are beginning to appear, such as the Cyber Security Forensics Analyst (CSFA) from the Cyber Security Institute.[18] Interestingly this qualification requires participants to complete a comprehensive practical examination, but it is also recommended that exam

[9] *M. K. Rogers, 'Computer forensics: science or fad', in Security Wire Digest, 2003, Volume 5, No 65. Available at http://www.cerias.purdue.edu/news/view/88*

[10] *J. Bates, 'Fundamentals of computer forensics' International Journal of Forensic Computing, 1999. Available on-line at http://www.forensic_computing.com.*

[11] *Association of Chief Police Officers, Good Practice Guide for Computer Based Electronic Evidence, (NHTCU, 2003). For the latest version, go to www.7safe.com/electronic_evidence/index.html.*

[12] *C. Everett, 'Forensics – cred or crud', Digital Investigation, 2005, Volume 2, No 4, 237 – 238.*

[13] *Institute of Computer Forensics Professionals – Code of Ethics available on-line at http://www.forensic-institute.org/code.html.*

[14] *D. J. Bagert, 'Texas licensing of software engineers: all's quiet for now' Communications of the ACM, 2002, Volume 45, No. 11, 92 – 94.*

[15] *J. C. Knight and N. G. Leveson, 'Should software engineers be licensed' Communications of the ACM, 2002, Volume 45, No 11, 87 – 90.*

[16] *Nigel Jones, 'Training and accreditation – who are the experts?' Digital Investigation, 2004, Volume 1, No. 3 189 – 194.*

[17] *https://www.isc2.org.*

[18] *http://www.cybersecurityinstitute.biz/.*

participants have 18 months experience before they attempt the exam. There are also certifications from commercial organisations for specific products.

In order to develop the autonomous standing of digital forensics, consideration should be given to the provision of a professional body and the issuance of a licence to practice. There is an expectation, as stated in principle number 2 of the ACPO Guidelines, regarding the competence of practitioners: "in exceptional circumstances, where a person finds it necessary to access original data held on a computer or storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions". Although the principle alludes to exceptional circumstances, the implicit expectation is that digital forensic practitioners should be competent before undertaking any computer forensic duties.

The Council for the Registration of Forensics Practitioners has begun to allow digital forensic practitioners to apply for registration, but there remains a question as to which is the most appropriate accrediting body for digital forensic practitioners. A significant factor that differentiates digital forensic professionals from other computing professionals is the possibility of acting as an expert witness. "Courts in the UK are taking an increasingly tough stance on expert witnesses who do not comply with their duties to the Court,"[19] and it is a requirement that digital forensic experts must demonstrate evidence of their competence to act as an expert witness.

Continuous professional conduct

Should an appropriate body be established, obtaining registration with the organisation ought to be the first step of establishing the professionalism of the member. Maintaining the professional conduct is a continuing process, and it will be necessary for continuous professional development. This process should include evidence of exhibiting the highest level of ethical behaviour at all times, and maintaining objectivity and confidentiality during an investigation. A practitioner has a moral responsibility to maintain their technical knowledge of the subject, and to conduct investigations with integrity. There is also an expectation that practitioners keep up to date and develop their skills and techniques in how they write up reports and explain their conclusions, as suggested by Casey.[20]

Consideration of Post Traumatic Stress Disorder

Although this section may seem somewhat out of context, there is a professional issue in dealing with the stress associated with working on digital forensic cases. It is important to realise that professionals working in digital forensics will come across cases that increase professional pressure, such as dealing with cases which have the potential to effect their work and their personal life – for example investigating paedophile or similar cases containing obscene materials. Constant exposure to such material may lead to the potential desensitising of the practitioner to the obscenity of such material, or even lead to practitioners suffering symptoms similar to post traumatic stress disorder. Tanner[21] discusses the potential of secondary trauma – particularly where digital investigators have to deal with cases involving pornography. Research undertaken for the Scottish Executive in 2005[22] indicated that incidents involving children or situations where events were interpreted as having high personal relevance, were identified as potential sources of stress. Unfortunately many digital forensics cases relate to the investigation of the creation and distribution of paedophile images.

Practitioner framework for professionalism in digital forensics

A suggested practitioner framework is outlined in this section. This framework is currently in development and is aimed at providing a practitioner framework for digital forensic professionals. The framework can be used in considering the abilities of practitioners and their suitability to be involved in particular cases and procedures (building on the ACPO Guidelines for Handling Digital Evidence). The framework will also include the duties and responsibilities outlined in the introduction of this paper. It is planned to develop this framework in the near future. The headings in the proposed framework include: Qualifications; Professional body membership; Accreditation; Certification; Consideration of legal, ethical and social concerns; Continued Professional Development; Reflective Review of Practice; and Promotion of the Discipline.

[19] *J. Ellison, 'The importance of being earnest – toughening up on experts', Forensic Accountant, 2005, Issue 28, summer 2005, 2 – 3.*

[20] *E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, (Elsevier Academic Press, 2nd edition, 2004).*

[21] *J. Tanner, (2006) 'Sex offenders and the Internet', paper delivered at Cyber crime Summit, Atlanta, Georgia http://www.cybercrimesummit.com /speakers/abstracts.htm#tanner.*

[22] *Claire Fyvie, Gill Moreton, Maggie Gray, Roslyn Law and Chris Freeman, 'Review of the occupational health support offered to Police Officers and staff fulfilling specific roles or tasks', (Government Social Research, 2006, N083/2006) available on-line at http://www.scotland.gov.uk/ Publications/2006/06/29114728/1 and http://www.scotland.gov.uk/ Publications/2006/06/29114728/0.*

The place of universities

Universities are able to contribute to the enhancement of professionalism in digital forensics by raising awareness and promoting professionalism. Universities have an important role in promoting digital forensics in the public domain and raising awareness about the strengths and issues associated with digital forensics and, indeed, computer crime. In addition, universities are in a position to provide education in digital forensics through the provision of undergraduate and post graduate programmes which cover the principles and techniques of digital forensics, and are accredited by relevant professional bodies and give graduates certification in digital forensics. If such programmes are developed, it will be necessary to obtain external validation and verification from independent bodies (for example from BCS or CRFP) in order to provide for appropriate standards, and to address the issues of accreditation and certification of digital forensic practitioners. It is important that universities work in collaboration with professional bodies, practitioners, police forces and legal experts to provide programmes that will address the needs of the industry in the provision of suitably skilled and certified experts.

In order to develop and sustain digital forensics as a discipline in its own right, the discipline needs to be supported by relevant research. Universities are in a position to develop the digital forensics research agenda (assuming funding is available) and can make a valuable contribution to the disciple by using expertise to undertake relevant research for the discipline. It is suggested that universities might usefully be involved in applied research in digital forensics, and that this applied research should be in collaboration with digital forensic practitioners and organisations in the public and private sectors.

As well as providing opportunities for education, universities are able to provide a co-ordinating role in helping to develop the discipline. There is an important role for academia in both research to assist digital forensic practitioners, and in educating and preparing future digital forensic specialists. It is suggested that universities should attempt to work together as a consortium – not in competition with each other – to develop the common body of knowledge and enhance the subject through collaborative teaching and research. Universities have the opportunity to provide a balanced and multidisciplinary view on the subject of digital forensics and can therefore provide a range of different perspectives on the relative merits of digital forensics.

Future development

The development of digital forensics as a discipline is likely to continue, at the very least, in the short term. Technical developments in operational procedures, in technology and digital forensic tools will be required in order to keep pace with developments in cyber crime. However, parallel developments in professional responsibility, certification and accreditation are required in order to maintain standards and the standing of the discipline.

Summary

This article has raised a number of the issues associated with professionalism, certification and accreditation in digital forensics. It is suggested that in order to maintain the credibility of digital forensics as a discipline, there is a need to raise the importance, and address the requirements, of professional issues in digital forensics. It is advocated that digital forensics practitioners will require suitable certification and accreditation in the future. The body which manages this process will need to embrace principles of self regulation as well as having the power and authority to provide the licence to practice and to bar from practice when necessary. There is a need to address and formalise the way the industry deals with professional and certification issues. It is suggested that in order to consider this further that professional bodies, practitioners, people involved in the criminal justice system and universities might usefully work together to produce a workable and manageable solution.

Alastair D. Irons is currently Associate Dean for Learning and Teaching in Engineering and Information Sciences (CEIS) at the School of Computing, Northumbria University. His current teaching and research is focussed on digital forensics, particularly in areas of professionalism and ethics. Alastair is a Fellow of the BCS and SEDA and sits on the Board of the North East Fraud Forum.

alastair.irons@northumbria.ac.uk

Anastasia Konstadopoulou is currently a Lecturer in Computer Science, Department of Computing, University of Bradford. Her research interest spans from interaction of mesoscopic devices with electromagnetic fields and applications to quantum technologies, to forensic computing and computer law. She was given the Nuffield award for Newly Appointed Lecturers in Science, Engineering and Mathematics in 2004.

a.konstadopoulou@bradford.ac.uk