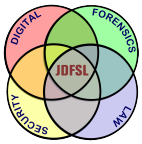

THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 1 | Number 4 Article 3

2006

Is Forensic Computing a Profession? Revisiting an Old Debate in a New Field

Bernd C. Stahl
De Montfort University

Is Forensic Computing a Profession? Revisiting an Old Debate in a New Field

Bernd Carsten Stahl
De Montfort University
Leicester, UK
bstahl@dmu.ac.uk

ABSTRACT

Forensic Computing is a new and quickly developing field. It is in the process of becoming an academic discipline or sub-discipline with all the features from full undergraduate and postgraduate course provision to conferences and journals. An important question in this process of turning into an established discipline is whether it will coincide with the recognition of the graduates as professionals. This paper hopes to stimulate the debate as to whether forensic computing is or should be a discipline. In order to approach this question, the paper will discuss the concept of forensic computing including the most salient topics of interest and the problems it has to contend with. This will lead to a discussion of the notion of professions and professionals, which will be expanded with a view to the debate on computing as a profession. Based on these considerations the paper will conclude by asking whether there is merit in promoting the debate on the status of forensic computing as a profession above and beyond the arguments already rehearsed for computing in general.

Keywords: forensic computing, profession, professional, ethics

1. INTRODUCTION

Computers and digital network are everywhere and affect most areas of life in western societies. They have the potential to emancipate us, to improve the reach of democracy or to widen the possibilities of education. They entertain us and help us communicate with others. At the same time, they can be misused, are important tools for modern criminals and can support all sorts of illegal and unsocial activities. The increasing importance of modern technology for crime has created a need for specialists who are able to understand these technologies and can discover legally viable evidence on them. This is a brief description of the field of forensic computing and of some of the possible tasks that practitioners in the field may encounter.

The field of forensic computing is relatively new as an academic discipline. Throughout the world universities and other educational institutions are undertaking to shape the specialists who will work in it. The field raises a variety of issues and questions, mainly due to its interdisciplinary nature and the fluidity of the environment in which it is developing. One interesting

question, the one that this paper will concentrate on, is what the status of the practitioners of forensic computing is or should be. Are forensic computing practitioners professionals, should they be or regard themselves as professionals, and what are the consequences of their being (or not being) professionals? These are the questions we will explore here.

The status of a professional is nothing new or specific to forensic computing. Debates about this status are centuries old, as are many of the arguments exchanged in such debates. This paper will therefore consider whether the field of forensic computing offers any particular or new aspects that would allow an answer to the above question. In order to explore the professional status of forensic computing, the paper will start out with a discussion of the field of forensic computing itself. Having thus provided an understanding of the content and problems of the field, we will continue with a discussion of the concept of professions and professionalism. This will include the purpose of professions as well as their downsides and problems. After establishing all the underlying concepts, the paper will then debate the applicability of the idea of a profession to forensic computing. The paper will end by asking how this debate will translate into practice and what can be done to help forensic computing develop in a desirable direction.

1.1 Contribution

This paper is conceptual and normative. It analyses the concepts involved, in order to discuss whether we can draw any conclusions from these. This research approach, which is also sometimes called "philosophical" (Jenkins, 1985), is necessary to lay foundations and allow for further research. The paper is more than a mere literature review in that it draws conclusions and suggests desirable developments. It is not an empirical paper but still claims to make a contribution to knowledge.

Given the complexity of the issues involved, the paper will concentrate on some specific fields. Geographically, the discussion will be limited to the UK. Such a limitation is necessary because our legal framework generally follows national borders. Regulations of professions will differ between jurisdictions. This is of course also problematic because the subject area of forensic computing is characterised by its international nature. The conclusions drawn here can therefore only claim validity within the UK legal framework. Further investigation into whether the conclusions drawn here are valid in other jurisdictions would be of interest but are beyond the confines of the paper.

Finally, the paper is explorative. It has been motivated by the observation that forensic computing displays some of the characteristics of a profession and the contrasting development of professionalism in computing in general. The paper will outline some weaknesses of the current debate and stimulate further discussion that will allow the practitioners of forensic computing to come to a conclusion whether they are or should be professionals and what consequences

such a professionalisation of the field would have.

2. FORENSIC COMPUTING

This paper will continue to use the term "forensic computing", rather than alternatives, such as computer forensics, digital forensics etc. This is a question of style rather than substance. The background is that the author lectures on a newly instituted undergraduate degree course called "Forensic Computing" at De Montfort University in Leicester, UK. Since these terms are all relatively new, there does not yet seem to be a very clear distinction between them. In a first attempt, one could define forensic computing as the "who, what, when, and how" of electronic evidence (Wall & Paroff, 2005 p. 1). It ostensibly addresses criminal matters related to computing or other new information and communication technologies (ICTs). In some respects forensic computing is therefore related to traditional forensic sciences. However, its close reliance on a specific type of technology sets it apart from these.

Forensic computing has as one important strand of activity the development of legally acceptable evidence. Since this requires a variety of skills and knowledge, it is in the process of becoming a new academic discipline (Broucek & Turner, 2004), which is also evidenced by the fact that its first academic journals, such as this one, have been created recently. There are journals such as "Digital Investigation", the "IEEE Transactions on Information Forensics and Security", the "International Journal of Digital Evidence" and there is a working group (11.9) of the International Federation for Information Processing that is called "Digital Forensics". In addition there are established related fields, notably security, where research in the forensic computing could be published. However, these developments are in their infancy. Compared with over 500 journals that publish IS-related work as registered on the website of the Association for Information Systems or compared with the thousands of outlets for medical or legal research, forensic computing cannot lay claim to professionalism in this respect.

The formation of this discipline is further hindered by the fact that the types of knowledge required for forensic computing are as diverse as the range of stakeholders interested in it. Stakeholders include privacy companies, governments, academia, the military, and the legal systems. These quite rarely communicate in depth and, in order for forensic computing to be successful, their traditional silo-mindset will have to be overcome (Rogers & Seigfried, 2004).

2.1 Topics of Forensic Computing

One way of approaching the field of forensic computing is to look at the topics it deals with. As indicated in the above definition, these topics will have something to do with the illegal use of ICT or with the use of ICT for illegal purposes. An important area of interest regarding such illegal activities has to

do with the intrusion into and the change of computer systems. This can be done knowingly as in the case of hacking (Broucek & Turner, 2004) or it can be done automatically through viruses, worms etc.

The area of hacking and intrusion into systems shows some of the fundamental problems of forensic computing. Among them there is the problem of drawing the line between legal and illegal acts, which partly overlaps with issues of knowledge. Does it count as hacking when I use someone else's password with their knowledge to check data? What if I do so without their knowledge? Is hacking defined as a problem because it causes damage or because it is a cyber-equivalent of trespass independent of any damage? Similar questions can be asked in the case of viruses. Are viruses bad per se, as the name may suggest (Klang, 2003) or are they only bad when they do damage? How is one to define a virus when many of its characteristics are shared with more benevolent software, such as autonomous agents?

While issues of intrusion and illegal / immoral use of technology may be the most obvious candidates for fields of interest to forensic computing, they are by no means the only ones. The topic that seems to be the one with the highest level of publicity is that of child pornography. While child pornography is by no means confined to ICTs, the use of technology has made the exchange of pertinent pictures much easier. A number of high profile cases of child pornography, combined with other crimes on children, which always generate huge public interest, have combined to shape the attention of forensic computing on these issues (Sommer, 2002). Again, there are a number of unclear issues, such as what constitutes pornography, who is a child, or why we prosecute some forms of behaviour and not others (cf. Levy, 2002). What is beyond doubt, however, is that child pornography is considered a serious social ill, by both the public and legislatures, and that it appears to be a central task of forensic computing to combat it.

In addition to such more spectacular issues, forensic computing will in many cases contribute to the fighting of conventional crime, which involves some aspect of ICT use. A typical example might be a drug dealer who holds contact details of customers or suppliers on a personal digital assistant or the use of programmable mobile phones for the planning and execution of other crimes. Forensic computing can also help fight crime where ICT has only been used in passing, thereby constituting a minor aspect of the overall forensic activities. Finally, forensic computing is likely to play a major role in the "war on terrorism". It seems obvious that modern terrorists make extensive use of ICT to prepare their attacks. They also use technology such as the internet to publicise their activities. Terrorists' leaving traces when doing so may open opportunities for forensic computing to support fighting terrorism.

2.2 Problems of Forensic Computing

While forensic computing has a variety of important topics and tasks to address

that have the potential to be of pivotal importance in the information society, it also has to contend with a variety of problems. The probably most important one in terms of this paper, which discusses issues of professionalism, has to do with the interdisciplinary nature of the field. In order to be able to produce useful digital evidence, which can be presented in a court of law, one requires knowledge from at least the technical and the legal domain. Both of these are large subject areas in their own right and both of them are moving quickly, albeit usually not synchronously. The interdisciplinary nature of forensic computing is thus one of its main problems.

A related problem is the quickly changing nature of the subject of interest, namely ICT. There are of course always new developments in all forensic sciences. However, their subject area itself is more or less stable. The fundamentals of a fingerprint have not changed in the last century, even though ways of recognising, storing or comparing it may have. Similar statements can also be made for newer forensic techniques, such as DNA analysis. In forensic computing, however, not only the tools and techniques are changing constantly, but also the very technology that is being investigated (cf. Sommer, 2002). Due to the fast pace of change, new techniques and procedures often cannot undergo a thorough scientific investigation and verification, which sheds doubt on their legal admissibility.

A variety of problems is created by questions of jurisdiction. Current ICT tends to be international or even global, whereas most laws are national. Much of the issues of interest to forensic computing, from child porn to terrorism, are global but if they go to court, investigators have to adhere to local regulations. Courts have to adhere to their national precedents, so that a chain of evidence that may be acceptable in one country may not be so in another. Also, local laws will often affect the availability of data. If a forensic computing investigator wanted to, say, establish a link between an online occurrence on the Internet and a specific person, then she would need to find out the IP address of the machine involved and be able to link this IP address to the person (Sommer, 2002). This may cause all sorts of problems due to dynamic assigning of IP addresses, multiple users on machines, etc. but even in the simplest case it will require information that is typically not held by law enforcement agencies but by other organisations, such as Internet service providers (ISPs) (Dinant, 2004). Whether this data is accessible depends on local regulations and requirements.

A related problem is that of the limits of possible action of forensic computing. One such limit that many authors agree on is that of privacy. Extracting electronic evidence will often hold the potential to find information that is not related to the cause of the investigation and it may lead to the collection of data related to other individuals apart from the one under investigation (Broucek & Turner, 2004; Poullet, 2004). There is no international agreement on what

constitutes privacy or what its limits are. An added problem is that such considerations will almost always take place in the context of a weighting privacy versus security. Again, there is no sign of an international consensus on how such judgments are to be made.

There are a variety of other problems that could be raised by forensic computing. These include the question of new problems created by forensic computing, such as network vulnerability through monitoring tools (Broucek & Turner, 2004). A more fundamental issue is the possible misuse of forensic computing as a rhetorical tool to promote particular ideologies. This paper will not be able to analyse these in depth but will conclude this section by asking what the characteristics of a forensic computing practitioner would be.

2.3 The "Forensic Computing Practitioner"

From what was said so far, one can deduce some of the skills or characteristics that a forensic computing practitioner would have to display. Considering these at this stage is useful because it will allow us to contextualise the subsequent discussion of professionalism in general. It will also facilitate the conclusion of the paper which will discuss whether forensic computing practitioner is or should be a professional and which consequences this would have.

The forensic computing practitioner will need a wide variety of skills. First of all, she will have to be an expert in her technical area of interest. As a minimum that will probably mean a good awareness of the theoretical and practical basics of computing, including hardware, operating and application software, and networking technologies. She should also be aware of current issues and trends, such as mobile phones, PDAs, or whatever else is current. She will have to have a good understanding of security issues, since her own work will require high standards of security but she will also have to be able to overcome security measures aimed at disabling investigatory activities.

Apart from this, she will need a good knowledge of the law. She will have to understand substantive as well as procedural law in her area of expertise. That means that she will have to know what constitutes a crime and what crimes can be committed with technology as well as what constitutes evidence and what has to be done to render evidence legally valid. In both of these fields, the practitioner will have to continually update her knowledge.

Apart from these core skills, the forensic computing practitioner will require a high level of reflective skills and personal integrity. This is partly caused by the unclear and often changing interplay between technology and the law. Cutting edge applications will often defy legal definitions which aimed at the preceding generation of technology. The practitioner must be able to extrapolate future developments from current ones. Furthermore, the activities in forensic computing will often involve sensitive ethical issues. Whether to release personal data, to look at information found on hard drives, share

knowledge with colleagues etc. may all require difficult ethical judgments. The practitioner must therefore be able to reflect on her position in society and make reasoned decisions. This is particularly true, since her skills lend themselves easily to misuse.

This issue of reflective awareness is exacerbated by the uncertainty of her employment situation. What was said about forensic computing so far assumed that the practitioner will work in law enforcement. A career in law enforcement is certainly something that students studying forensic computing have in mind. Another career might be as an expert witness. Expert witnesses need similar skills to law enforcement officers but their roles are of course quite different. Where law enforcement seeks convictions and are thus partial in a court of law, expert witnesses need to be neutral. In both cases one can nevertheless make the (probably simplistic) assumption that her work in general is justified and will serve the greater good of society. It is not likely, however, that all students of forensic computing will end up in law enforcement. Their specific skills will make them interesting candidates for employers in other sectors. They would, for example, be useful additions to teams concerned with security. In the case of private employment, the question of use and misuse of her skills becomes even more pronounced. It is quite possible that employers would like information about their employees or other information technically available to the forensic computing practitioner, which she possibly should not give them for a variety of reasons. This means that the ethical onus to make decisions is even more important. At the same time it means that new legal issues may arise, for example from employment law, which requires the ability to research and understand such questions independently.

Having said so much about the forensic computing practitioner, we can proceed to ask the question whether she is or should be a professional. In order to answer the question, it will be useful to discuss the concept of professionals and professionalism

3. PROFESSIONS AND PROFESSIONALISM

This section will discuss the meaning of the terms profession or professionalism as well as some of the advantages and disadvantages of professions. The traditional professions such as lawyers or medical doctors are quite old and much can be said about them that this paper will not be able to cover. The current discussion will therefore concentrate on the well-discussed issue whether computing should be a profession. This is a useful approach to our question because forensic computing is clearly closely linked to computing in general and many of the potential forensic computing professionals are already computing professionals (if computing is a profession). Because of the large overlap of the two fields, the majority of the arguments used for computing will also be applicable for forensic computing. Forensic computing is a special case of computing which creates some specific issues which

warrant a more specific debate**.**

3.1 The Concept of a Profession

The term "profession" comes from the Latin words "pro", meaning before and "fateor", meaning to avow. A literal translation might thus refer to a covenant or to vow to be faithful (Mason et al., 1995). The original use of the word therefore aims at fidelity to a religious order. It was broadened to capture a calling or occupation. This has developed into a reference to being licensed by a governing agency, which authorises the professional's practice and has close control over possible activities (Gleason, 2002). Modern day professions are characterised by a variety of features. These tend to include specific knowledge of a clearly defined field, a large measure of autonomy, formal organisations, codes of conduct or ethics, and other social functions (Johnson, 2001). Mason et al (1995) emphasise that the knowledge of relevance in a profession is more than manual know-how and that it typically has a strong theoretical side. Professions also take a wider view of their subject area and tend to claim social responsibility and general awareness of the results of their activities.

Professions are constituted by professionals. These tend to share some characterising features. A central one of these specific features is the fact that they tend to have a specific education, which, in most cases, results in a university degree. However, most professions require more than just theoretical book knowledge. An important aspect of professional education is a lengthy "apprenticeship" where prospective members have to undergo practical training under the close supervision of established members of the profession. Only such a specialised education allows them to master the body of knowledge concerned with the purpose of the profession (Spinello, 1997). Their high degree of knowledge and the specialised nature of the subject matter allow professionals to develop a high degree of autonomy. This is closely linked to a high status and recognition by the public, which, in turn, tends to be reflected by high remuneration.

The professional has a strong position vis-à-vis his or her clients (Weckert & Adeney, 1997) who tend to be in a position of vulnerability. This means that professionals must look beyond the immediate working relationship and must consider the greater good of society (von Weltzien Hoivik, 2002). Professionals are therefore characterised by a clearly defined role responsibility which is linked to a variety of positive sanctions (money, status) but also require a high level of commitment. Such roles are therefore linked to voluntary uptakes and are not typically given to individuals who do not desire them or are not qualified (May, 1992).

3.2 The Purpose of Professions

The question why a society would wish to promote professions refers directly to their definition. It has something to do with the specialised knowledge and

the exposed statue of the individuals who hold the prerequisites to become professionals. The critical expertise held in professions requires some sort of control if society wants to avoid a situation where such expertise is subject only to market forces and professionals are merely "guns for hire" (Johnson & Mulvey, 1995 p. 63). Professions are thus meant to regulate the special power relationship between professionals and their clients. Looked at from this point of view, the purpose of professions is primarily of a moral nature. Society regulates a relationship between strong and weak individuals by creating a governing body, the profession, which supervises the behaviour of the strong.

There are also other purposes a profession can fulfill. A very important one is the guidance of its members. Professions can use a variety of means to guide professionals to act in ways which are perceived to be compatible with the purpose of the profession. A central approach, which can be found in one way or other in most professions, is to develop and enforce a code of conduct or ethics. Such codes can be seen as guidelines which allow the individual professional to sharpen their understanding of what is required of them. More importantly, they can serve the function of allowing the profession to represent such expected behaviour to third parties. If, for example, a professional comes into a situation where she is under pressure to act in ways that she believes to be incompatible with the expectations leveled at a professional, then she can point towards a publicised code which renders it easier to stand up to such pressure.

Another important task of professions is to act as a representative of professional interests in society. They publicise the relevance of the task a professional is charged with and serve as negotiator on behalf of the professionals. They thereby try to attain the advantages linked to professions for the professionals and collaborate with other groups on setting professional standards. They symbolise and uphold such standards to the outside and enforce them to the inside. Professions are thus mediators between state and society and the individual professional.

3.3 Downsides of Professions

Professions are an important aspect of modern societies with a high degree of division of labour. They guarantee the working of specialised relationships. One should be aware, however, that there is also a large amount of criticism of professions. One aspect of such criticism refers to the fact that professions can only have the beneficial effect they are meant to have in a society which has a citizenry which has a basic understanding of the subject matter and its importance (Johnson & Nissenbaum, 1995).

Another problem has to do with the status of professionals in modern organisations. As we have seen above, a classical characteristic of professionals is their independence and autonomy. These features are of decreasing importance even in the classical professions such as law and

medicine. They are even more problematic for newer professions such as engineering, whose practitioners tend to be employees in large commercial organisations. The ethical imperatives of professions must compete with the commercial imperatives such professionals face and, if there is a conflict of interests, it is likely that the professional requirements will be of secondary importance (von Weltzien Hoivik, 2002). Professions are there to facilitate moral behaviour in the case of conflicts of interest but it is not clear how far they can do this if the professional is a member of an organisation and must rely on continued employment to gain her livelihood.

More important than these issues of implementation and effectiveness of professions are attacks on their very idea. There is a range of voices who are fundamentally critical of the notion of professions per se, mostly because they automatically have less desirable effects, which can be more relevant than their advantages. Newton (1998) distinguishes between the Harvard and the Chicago School of sociology with regards to professions. The Harvard school represents the view of professions as introduced so far, concentrating on their intrinsic importance and the relevance of education. The Chicago School, on the other hand, views professions primarily as barriers to market entry. Indeed, there does not seem to be a contradiction between these two views. In order for a profession to be able to enforce the moral standards it has set, it must be able to preclude individuals from practicing, which effectively constitutes a barrier to market entry. At the same time, the high salaries received by traditional professionals such as lawyers and medical doctors suggest that competition in their markets is limited which gives the professionals a high negotiating power.

Society is therefore well advised to consider whether the tasks which are undertaken by the members of a profession are of such importance as to warrant the institution of a profession (Kultgen, 1998). If there is no higher public good involved, then the society may be better off not regulating matters and thus not privileging some, who are usually part of the privileged sector of society in the first place.

3.4 Computing: A Profession?

While some professions have been established for a long time, there are some new fields of activity for which the question whether they constitute a profession is open. Computing is one such field with obvious relevance for this paper. It is open to debate whether forensic computing is a sub-speciality of computing in general or whether it is a new, albeit related, field. Either way, the discussion whether computing is a profession has bearing on the same question for forensic computing.

Some authors contend that computing practitioners typically view themselves as professionals, that they publish in specialist outlets and use a specific jargon (Oz, 1992). It is probably nevertheless fair to say that computing is not (yet) a profession comparable to the established professions like law and medicine. It

is less clear why this is the case. There are certainly some parallels. Computing has established a body of knowledge and has become an academic discipline. However, in order to become a computing practitioner one does not necessarily have to have gone though an academic education and it is (or at least was until a few years ago) relatively easy to join computing with a non-computing background. In fact, the quick growth of the computing industry during the 1990s meant that a large percentage of computing practitioners had a different background.

Another reason why computing is probably not truly a profession is that there are no professional bodies with statutory powers. There are of course professional organisations for computing personnel, such as the British Computer Society or the Association for Computing Machinery. These do fulfil a considerable part of the tasks of professions described above. They discipline their members, create ethical guidelines and serve as intermediary between society in general and their individual members. They differ from other professional bodies through their lack of formal powers. Nobody needs to become a member of any of these organisations in order to work in computing. They may give prestige and legitimacy but for the vast majority of jobs they are not obligatory. This differs sharply from the medical or legal professions where it is typically a condition of employment to be a member of the statutory bodies, which represent the profession. Accordingly, they tend to be strongly regulated by the state, which again is not true for the computing professional bodies (Forester & Morrison, 1994).

An interesting question is why this is the case. One obvious answer would be that computing is simply too young a discipline to have developed all the characteristics of a fully-fledged profession. To some degree this is certainly true. Computers are barely 60 years old and their social relevance has only become pervasive in the industrialised world in the last 20 or so years. Technology evolves constantly at high speed and it is not always clear what should be considered part of computing. Indeed, the very choice of word "computing" may be misleading because many of the cutting edge technologies of social relevance involving ICT may be found in other disciplines from engineering to bio-technology. The question thus arises: who should be considered a computing professional and how are such definitions to be developed and maintained?

Another, less obvious, reason for the lack of a clearly recognised computing profession may be the lack of a public perception of a need for it. We have seen that the unequal and ethically charged relationship between professional and client is a major reason for the creation of professions. Such a relationship does not exist in an obvious form in computing. Most programmers or computer scientists are members of commercial organisations or work independently. They rarely deal directly with individual customers or end

users. Where they do, the negotiating position tends to be more equal and competition is strong. They therefore do not have the privileged position of power of a doctor or lawyer. The ethical issues involved in computing are thus much less obvious and in need of regulation. While there can be little doubt that computing has ethical relevance, the academic field of information and computer ethics attests to this, there may be other ways of dealing with these, apart from professionalisation. The responsibilities of computing practitioners may be discharged in the same way we all deal with our responsibilities to society. It is sometimes pointed out that the impact of the activities of computing is such that it requires a higher than usual measure of responsibility (Rogerson, 1998; Johnson, 2001; Buchanan, 2001). It is not necessarily clear that these issues are of sufficient importance to warrant the social and economic costs of creating a traditional profession. Engineering, as a closely related discipline, shows that a longer history of a discipline does not have to lead to the development of a profession.

4. FORENSIC COMPUTING: A PROFESSION?

The above arguments concerning computing in general apply to a large degree to forensic computing as well. Forensic computing cannot currently count as a profession. It lacks standards, peer review, and professional certification (Meyers & Rogers, 2004). The question is whether there are significant differences between computing and forensic computing that would warrant the institution of a profession in the latter even if it is still lacking in the former. At the current stage there are professional bodies, which accept forensic computing practitioners as members. However, they tend to be existing bodies of forensic sciences that are extending their interests to computing. In the UK, for example, there is the Council for the Registration of Forensic Practitioners (http://www.crfp.org.uk/), which admits computer forensics specialists, but there is no legal requirement to become a member to fulfil any official role.

Forensic computing is currently even less clearly defined than computing. The creation of digital evidence is an activity that some police forces are specialising on and in which they have developed considerable expertise. However, there are a number of individuals outside of law enforcement who are involved in forensic computing. Some people serve as expert witnesses in legal cases and there are academic researchers who investigate issues of relevance to forensic computing. Many individuals are specialising in the development of digital evidence in the private sector, whether for security, management purposes or others.

There are thus many individuals who could form the nucleus of a new profession, if we collectively thought it would be a good idea to have one. The question is whether we should think so. Looking at the purpose of professions as protecting the public and ascertaining acceptable behaviour by highly ranked specialists, it seems quite clear that forensic computing should be a profession.

The forensic computing practitioner has a strong institutional position, be it as a member of law enforcement or in the private sector. Society may therefore desire a clear codification of her behaviour and enforcement mechanisms to ensure adherence to set standards.

Forensic computing also fulfils the requirements of the individual professional. A potential forensic computing professional requires fluency in a wide body knowledge and the ability to do independent research and develop an understanding of new and changing fields. This means that the professional will need an academic education, even though it is currently not too clear what exactly the content of this education should be. The creation of a profession would therefore be helpful in that it would force a discourse on the required content of education. This does not mean that there needs to be one standard curriculum, but it would be helpful if there were a professional body that could guide universities in making a decision as to how much legal, professional, technical, or other topics should be included in a curriculum.

We have also seen that the autonomy and independence which typically characterise professionals are important because they increase the probability of the professional encountering ethical problems. Such ethical issues are all but guaranteed to arise in the course of activity of forensic computing. The mix of illegal activities with the ability to access data that is by definition not meant to be accessed, create an environment where problems are bound to arise. As indicated earlier, privacy is generally seen as a central issue for forensic computing. How is the individual to behave if there is a chance that confidential data may be viewed, while, at the same time, there may be some sort of illegal activity ongoing? A related issue is that in many cases it will not be possible to confine investigations to the data of just one individual. When reading email or log files, it is bound to happen that data of individuals will be exposed who had nothing to do with the individual investigation. Data protection regulation may offer an initial orientation but it will rarely suffice to disentangle the difficult ethical issues involved.

Another good reason for the creation of a profession is the protection of the individual professional. As indicated above, most of the considerations of forensic computing concern issues of law enforcement and imply that the professional will work for the police or other law enforcement agencies. It is quite possible, however, that someone with the qualification as a forensic computing professional will find employment in the private sector, where requirements may be quite different. The specialised knowledge the professional holds renders her a primary subject for conflicts of interests. An employer wanting to spy on an employee would be very happy to have a forensic computing specialist in their employment. We are then entering the difficult issue of surveillance in the workplace (Stahl et al., 2005). This will create the grounds for possible ethical dilemmas which the individual will find

difficult to navigate. A profession may not be a panacea for such situations but it may provide a solution for relatively straightforward and expectable cases.

There is thus a strong case to be made for forensic computing to become a profession, independent of the status of computing as a whole. Forensic computing has more complex educational requirements, will produce more powerful individual practitioners, will require social control and ethical guidance, and will be easier to abuse than computing in general. Creating a profession therefore would seem to be desirable. Having come to such a conclusion, one should also admit that it would be fraught with problems.

One of these problems is the question how the profession should be defined. It is foreseeable that existing professional bodies would compete regarding the creation of this new profession. Should it be seen primarily as a legal profession or as a technical? How is the decision to be made? Depending on the outcome of this question, the educational content of forensic computing will differ greatly. The definition of the body of knowledge also produces other problems. Is there really anything that all individuals concerned with issues of forensic computing have in common? Or, if not, do we possibly need more than one profession? This question of the body of knowledge is a recurring theme in the literature on forensic computing. While there is general agreement that forensic computing professionals would need technical as well as legal and social skills, there is little agreement what this should include in detail. One of the problems seems to be that the academic community seems to be interested in different issues than the professional one (Yasinsac et al., 2003).

Another difficult issue is that of national jurisdiction. The digital crime which is the primary interest of forensic computing is by definition international. A hacker or a paedophile can simply use the Internet to move activities and traces across borders. Pornography, including child pornography, is a good example of the problems arising due to jurisdictional issues. What is legal in one country will be illegal in another. The example of the USA shows that even within the country there is little agreement on what should be illegal. There are open questions regarding the age of consent, the admissibility of homosexuality, of bestiality, and others. All of these have to do with local morality which raises the fundamental problem of whether there are any rules that apply to all of humanity without distinction (Stahl & El-Beltagi, 2004). How is a profession to navigate these difficult issues? Relying on local preferences may render the moral problems manageable but goes against the international and intercultural nature of the technology in question.

Apart from this, there are many practical issues to consider. How is the practical training of forensic computing professionals to be organised? Will they have to be licensed? If so, what are the criteria? How can bureaucracy be minimised while still guaranteeing the international viability for the qualification as forensic computing professional? How can we avoid that

forensic computing will become a vehicle for particular interests (Kenneally, 2002)? All of these are questions go far beyond what a single paper can discuss. If the arguments put forward in this paper are accepted, however, then we need to start thinking about them. A new journal such as the Journal of Digital Forensics, Security and Law, catering for the individuals with a stake in forensic computing, should be a good place to carry this debate. I hope that this paper will help promote the discussion and help create a sound foundation for a future profession of forensic computing.

5. REFERENCES

Broucek, Vlasti & Turner, Paul (2004): Intrusion Detection: Issues and Challenges in Evidence Acquisition. In: *International Review of Law, Computers & Technology* (18:2): 149 - 164

Buchanan, Elizabeth A. (2001): Ethical Considerations for the Information Professions. In: Spinello, Richard A. & Tavani, Herman T. (eds.) (2001): *Readings in Cyberethics*. Sudbury, Massachusetts et al.: Jones and Bartlett: 523 - 534

Dinant, Jean-Marc (2004): The Long Way from Electronic Traces to Electronic Evidence. In: *International Review of Law, Computers & Technology* (18:2): 173 - 183

Forester, Tom & Morrison, Perry (1994): *Computer Ethics - Cautionary Tales and Ethical Dilemmas in Computing*. 2nd edition, Cambridge, Massachusetts / London: MIT Press

Gleason, David H. (2002): ICT Professionalism. In: Alvarez, Isabel et al. (eds.) (2002): *The Transformation of Organisations in the Information Age: Social and Ethical Implications*. Proceedings of the sixth ETHICOMP Conference, 13 - 15 November 2002, Lisbon, Portugal. Lisbon: Universidade Lusiada: 113 - 124

Gotterbarn, Don (2004) On Licensing Computer Professionals. In. Bynum, Terry & Rogerson, Simon (eds.) (2004): *Computer Ethics and Professional Responsibility*. Blackwell: Oxford, 157 – 164

Jenkins, Milton A. (1985) Research Methodologies and MIS Research. In: Mumford, Enid; Hirschheim, Rudy; Fitzgerald, Guy & Wood-Harper, Trevor (eds) (1985): *Research Methods in Information Systems* (IFIP 8.2 Proceedings). Amsterdam: North-Holland: 103 - 117

Johnson, Deborah G. (2001): *Computer Ethics*. 3rd edition, Upper Saddle River, New Jersey: Prentice Hall

Johnson, Deborah G. & Mulvey, John M. (1995): Accountability and Computer Decision Systems. In: *Communications of the ACM* (38:12): 58 - 64

Johnson, Deborah, G. & Nissenbaum, Helen (1995): What is Computer Ethics? In: Johnson, Deborah G. & Nissenbaum, Helen (eds.) *Computers, Ethics & Social Values*. Upper Saddle River: Prentice Hall: 1 - 15

Kenneally, Erin (2002): Computer Forensics: Beyond the Buzzword. In:*;login:* (27:4): 8 - 11

Klang, Mathias (2003): A Critical Look at the Regulation of Computer Viruses. In: *International Journal of Law and Information Technology* 11: 162-183

Kultgen, John (1998): The Ideological Use of Professional Codes. In: Stichler, Richard N. & Hauptman, Robert (eds.) (1998): *Ethics, Information and Technology: Readings*. Jefferson, North Carolina: MacFarland & Company: 273 - 290

Ladd, John (1995): The Quest for a Code of Professional Ethics: An Intellectual and Moral Confusion. In: Johnson, Deborah G. & Nissenbaum, Helen (eds.) (1995): *Computers, Ethics & Social Values*. Upper Saddle River: Prentice Hall: 580 - 585

Levy, Neil (2002): Virtual Child Pornography: The Eroticization of Inequality. In: *Ethics and Information Technology* (4:4): 319 - 323

Mason, Richard O.; Mason, Florence & Culnan, Mary J. (1995): *Ethics of Information Management*. Thousand Oaks, London, New Delhi 1995: SAGE

May, Larry (1992): *Sharing Responsibility*. Chicago: University of Chicago Press

Myers, Matthew & Rogers, Marc (2004): Computer Forensics: The Need for Standardization and Certification. In: *International Journal of Digital Evidence* (3:2): 1 - 11

Newton, Lisa (1998): The Origin of Professionalism: Sociological Conclusions and Ethical Implications. In: Stichler, Richard N.& Hauptman, Robert (eds.) (1998): *Ethics, Information and Technology: Readings*. Jefferson, North Carolina: MacFarland & Company: 261 - 272

Oz, Effy (1992): Ethical Standards for Information Systems Professionals: A Case for a Unified Code. In: *MIS Quarterly* 16: 423 - 433

Poullet, Yves (2004): The Fight against Crime and/or the Protection of Privacy: A Thorny Debate! In: *International Review of Law, Computers & Technology* (18:2): 251 - 273

Rogers, Marcus K. & Seigfried, Kate (2004): The Future of Computer Forensics: A Needs Analysis Survey. In: *Computers & Security* (23:1): 12 - 16

Rogerson, Simon (1998): *Ethical Aspects of Information Technology - Issues for senior executives*. London: Institute of Business Ethics

Sommer, Peter (2002): Evidence in Internet Paedophilia Cases. In: *Computer and Telecommunications Law Review* 8: 176 - 184

Spinello, Richard (1997): *Case studies in information and computer ethics*. Upper Saddle River, NJ: Prentice Hall

Stahl, Bernd Carsten; Prior, Mary; Wilford, Sara & Collins, Dervla (2005): Electronic Monitoring in the Workplace: If People Don't Care, then What is the Relevance? In: Weckert, John (ed.): *Electronic Monitoring in the Workplace: Controversies and Solutions*. Idea-Group Publishing, Hershey PA: 50 - 78

Stahl, Bernd Carsten & El-Beltagi, Ibrahim (2004): Cultural Universality versus Particularity in CMC. In: *Journal of Global Information Technology Management* (7:4): 47 - 65

von Weltzien Hoivik, Heidi (2002): Professional Ethics - a Managerial Opportunity in Emerging Organizations. In: *Journal of Business Ethics* 39: 3 - 11

Wall, Christopher & Paroff, Jason (2005): Cracking the Computer Forensics Mystery. In: *The Computer & Internet Lawyer* (22:4): 1 - 6

Weckert, John & Adeney, Douglas (1997): *Computer and Information Ethics*. Westport, Connecticut / London: Greenwood Press

Yasinsac, Alec; Erbacher, Robert F.; Marks, Donald G.; Pollitt, Mark M. & Sommer, Peter M. (2003): Computer Forensics Education. In: *IEEE Security & Privacy* (1:4): 15 - 23