

Chapter XIII

Forensic Computing: The Problem of Developing a Multidisciplinary University Course

Bernd Carsten Stahl, De Montfort University, UK

Moira Carroll-Mayer, De Montfort University, UK

Peter Norris, De Montfort University, UK

Abstract

In order to be able to address issues of digital crime and forensic science in cyberspace, there is a need for specifically skilled individuals. These need to have a high level of competence in technical matters, but they must also be able to evaluate technical issues with regards to the legal environment. Digital evidence is worth nothing if it is not presented professionally to a court of law. This chapter describes the process of designing a university course (a full undergraduate BSc degree) in forensic computing. The aim of the chapter is to present the underlying rationale and the design of the course. It will emphasise the problem of interdisciplinary agreement on necessary content and the importance of the different aspects. It is hoped that the chapter will stimulate debate between individuals tasked with designing similar academic endeavours and that this debate will help us come to an agreement what the skills requirement for forensic computing professionals should be.

Introduction

The fact that cyberspace increasingly is turning into a place where criminal acts are committed requires law enforcement agencies, businesses and other organizations to develop new competences. This means that either existing personnel will have to develop new skills or that new personnel with specific skills will have to be employed. These alternatives require facilities that allow people to learn the skills required for dealing with computer crime and digital evidence. The evolving sophistication of computer crime, together with the methods and tools required to detect and deal with it, demand the timely development of new university programs. It is the purpose of this paper to recount the development of a new undergraduate course¹ in forensic computing in the School of Computing of De Montfort University, Leicester, UK (DMU). The paper will start by providing a general background of the rationale for starting the course. It will go on to describe the requirements and organizational constraints that shaped the outline of the course. The paper will then overview the topics to which students must be exposed in order to discharge their professional responsibilities. Finally the paper will discuss the implementation of the forensic computing course and reflect upon the problems arising due to its complex and multi-disciplinary nature.

The paper should prove interesting to readers of the book for several reasons. Among these is the fact that the chapter moves beyond the theoretical and academic discussion to deal with the important question of how forensic computing can be taught with requisite emphasis upon the practical, legal, and ethical issues to which it gives rise. The paper raises the problem of where those professionals with the skills necessary to address the issues of forensic computing will come from and of how a university can deal with the challenge of setting up and teaching degree courses in the field. More importantly, the paper reflects upon the interdisciplinary nature of forensic computing and the problems to which this gives rise in the design and delivery of forensic computing courses. Competition for resources between the technical, legal, and professional components of the degree is generated by the complexities of forensic computing. Which skills and to what degree are these needed by a high-technology crime investigator? How much technological knowledge is necessary and how much knowledge of the law does a forensic computer scientist need? Who can count as an expert witness in a court of law? These questions lead to greater questions: What is the role of computers in society, the function and purpose of the law, and ultimately to the deep question of how may we, as societies, design our collective lives. While we cannot answer these questions comprehensively here, it is important to stress the role they must play in the development of a successful forensic computing course.

Rationale of Introducing Forensic Computing at De Montfort University

Since the end of the dot.com boom, student interest in computing and related disciplines has noticeably declined. One answer to this problem is to recruit students to innovative and more exciting courses. The current attempt to design a course in forensic computing is one example of this drive to diversify the teaching portfolio of the DMU School of Computing.

Forensic computing, in the imagination at least, carries the promise of excitement redolent of TV series and thrillers. Whatever the reality, the enthusiasm thus engendered, no less than that derived from intellectual propensity, should be harnessed by universities in both their own and society's interests. Several universities in the UK have set up courses related to forensics in the last few years. The School of Computing at De Montfort University is running a course in forensic science, which has managed to attract students against the general tide of disinterest in and lack of recruitment to science studies noted nationally.

Given the ubiquity of computing and other forms of information and communication technologies in modern societies, it is not surprising that these technologies are used for criminal purposes. Consequently, the police need to be able to investigate ICT and they need to be able to present their findings as evidence in courts of law. Since the DMU School of Computing has substantial experience teaching and researching various aspects of ICT, it seems a sensible choice to offer a course that will specifically satisfy these demands.

Moreover, DMU as a new university (that is one of the UK universities that were polytechnics and were elevated to university status in 1992) prides itself in being professional, creative, and vocational. Accordingly the teaching portfolio aims to be applied and practical, unswervingly directed towards the provision of graduates with the skills required by employers.

In the case of forensic computing, there are two main areas of possible employment. Firstly, the police force with its need to develop high technology crime unitsⁱⁱ, and then the private companies that wish to deal with a variety of illegal behavior involving their technology. Both areas are predicted to grow quickly in the coming years and it is expected that the job market for graduates skilled in forensic computing will grow concomitantly. These predictions are corroborated by the local high-technology crime unit of the police as well as by market research conducted by the marketing department of De Montfort University. Most importantly, the marketing department predicted that there would be ample interest by students in the course. These reasons were sufficient to persuade the university to start designing the course and to offer it to students.

Competitor Analysis

In order to be sure that the course would be viable and would be able to cater to a market that exists but is not already saturated, the course team undertook a competitor analysis. At undergraduate level for UK 2005 entry, UCAS (the UK Colleges Admission Service) listed three competitors in July 2004 when detailed course design was initiated. At the point of preparation of this document (April 2005), this had risen to four with the addition of Sunderland. None of these institutions is geographically close to dmU and so offered minimal direct competition for applicants who want to stay close to home. On a content level, the planned course was set apart by a strong presence of digital evidence handling within the professional context of forensic investigation. A brief overview of the competing courses can be found in Table 1.

There is thus a small but growing market for forensic computing in the UK. We did not consider the international competition for several of reasons. Firstly, most of our students are UK students and, at least initially, we expect that students will make a rather ad hoc decision to enter the course. Such a decision in our experience tends to be rather

Table 1. Other university courses in forensic computing offered in the UK

Institution	Award	Summary (<i>edited from web site</i>)
Huddersfield	BSc(Hons) Secure and Forensic Computing. G603 3yr FT 4yr SW 20 places	This course is a 4 year sandwich (or 3 year full time) programme designed to produce computer professionals with the skills required to design and develop computer systems secure against unauthorized access and criminal manipulation, evaluate existing computer systems in terms of their security, and investigate computer based crime presenting evidence to a standard required of a criminal court.
Staffordshire University	Forensic Computing BSc/BSc Hons FG44 (4yr SW) FGK4 (MEng 5yrSW) also joint with various others	This award attempts to give you the knowledge and skills to enable you to prevent, repair and detect the causes of data corruption, loss or theft.
University of Central Lancashire	BSc(Hons) Computing (Forensics) GF44 3yrFT	Forensic computing is about detecting, preserving and presenting evidence of computer crime.
University of Sunderland	Forensic Computing 3 year full-time Degree, 4 year sandwich Degree	BSc (Hons) Forensic Computing is designed for those wanting to study and develop skills in forensic data computing. The degree provides an understanding of criminology, types of forensic data and appropriate analysis techniques, and how to operationalise findings in decision support software based upon advanced artificial intelligence technologies and 'industry entrance level' computer programming skills.

local than international. Secondly, forensic computing is closely linked to the legal and regulatory system and we can only claim expertise in areas of forensic computing in the UK. Questions of the legal framework, including requirements for the handling and presentation of evidence may be different in other legislations, which means that professionals active in the UK need to know the UK model. We realize that this may turn out to be a problematic assumption in the light of the international nature of ICT and related misuse and crime. We may have to revisit this problem but it did not influence our initial design of the course.

A possible alternative to a full three to four year BSc course might have been a one or two year postgraduate degree. There are a number of such top-up options available in the UK and elsewhere. We did not choose to follow this route because we believe that the amount of material— technical, legal, and professional, that needs to be mastered in order to be a successful professional in forensic computing is such that it deserves to be taught in a full first degree course. However, if our BSc turns out to be a success and attracts a large number of students, then we will consider offering a follow-up postgraduate option.

Requirements

In order to perform a useful requirements analysis for the course we concentrated on the potential employers of our students and asked what they would wish their employees to know. The two main employers are expected to be the police and security/IT departments in commercial organizations. These have distinct but partially overlapping needs and interests and it is therefore important to distinguish between the different sets of requirements.

The police require expertise in forensic computing for the purpose of identifying, trying, and convicting criminals. This refers to specific computer crime but also to general crime that is committed with the involvement of ICT. Today nearly every crime that is investigated byⁱⁱⁱ the police involves digital media (Janes, 2005). Computer crime includes matters such as hacking into systems, online fraud etc. (Tavani, 2001). The advent of broadband has attracted unprecedented numbers of hackers and botnet herders involved in the commission of increasingly sophisticated crimes (Deats, 2005). In general crime ICT is used for many purposes. These include for example the storing of drug dealers' customer data on mobile telephones and the e-mailing of threats by murderers to their victims. While the use of technology for the purposes of finding evidence is indispensable to the police force, and while it is increasingly involved in the commission of crime, computer-based evidence is useless unless it is collected and presented in court in such a way that it will not contravene the rules of admissibility and will lead to the successful conviction of criminals. The collection and presentation of computer evidence is therefore a technical matter that must nonetheless be undertaken in strict compliance with legal rules. This duality in the purpose and nature of computer forensics means that experts, especially those involved with law enforcement, must be trained to quite literally look both ways simultaneously.

The goals of business organisations in employing forensic computing experts often differ from those of the police. Businesses incline to the quiet detection and prevention of outside attacks as well as internal misuse. Forensic computing can be helpful in detecting and following up attacks and in determining and documenting the misuse of systems for future reference. Issues of risk management, avoidance of legal liability (Straub & Collins, 1990) and issues of productivity loom large in the annals of computer forensics in the commercial field. Research indicates that the main threat to business originates from employees and that the use of ICT for non work-related purposes is very problematic. A number of terms have been developed by businesses to describe these unauthorised activities, “cyber-slacking” (Block, 2001, p. 225), “cyberslouching” (Urbaczewski & Jessup, 2002 p. 80), or “cyberloafing” (Tapia, 2004 p. 581). The investigation of employee misuse of ICT by employers is often satisfied employing lower standards of evidence collection and presentation than that required by the police force. This is because employers are often content to dismiss recalcitrant workers and in any case prefer not to attract attention to adverse behaviour in the workforce. This does not mean however that computer forensics conducted in the workplace should be with a blind eye to legal requirements; a wrongful dismissal suit may be grounded on a lack of respect for privacy, avoidable had the legal rules of forensic computing been observed. Figures released for the first time by the National High Tech Crime Unit (UK) show that the value of losses suffered as a result of commercial e-crime in 2004 alone stand at £2.4bn. For this reason alone, forensic computing within the commercial context will have to be increasingly tailored to take account of the law.

This brief résumé of the requirements of the two main groups of potential employees indicates that it is otiose to tailor the course specifically for computer forensics in either one or the other group. Students of computer forensics, regardless of their destination should be equally well-versed in technical and legal matters.

Given the fast pace of change in the field of computer forensics, one can safely assume that the technologies we teach to our students in the first year will be outdated and forgotten (at least by criminals) by the time they graduate. Students should therefore be able to continuously educate themselves as to changes in the technology and in the procedural and substantive law relevant to their field. It is clear that students must be taken to the wide horizon of computer forensics to understand the technical, legal, ethical, and societal aspects of their role as experts in forensic computing. This leads us to the question of how the different skills can be implemented.

Implementation of the Course

This section will explain how we planned the delivery and structure of the course in order to address the skills requirements indicated above. It will therefore explain the content and purpose of the course structure that can be found in the appendix. As can be seen from the appendix, all of the modules to be taught in the first two years of the course are 30-credit modules. That means that they are taught over a whole year and typically have a contact time of three or four hours per week. The assumption is that students should

spend about ten hours per week on each module. The modules are assessed by a mix of coursework and examination, depending on the specific outcomes being assessed. All students will be expected to do a placement year during their third year of study. Placements consist of work in a company or other organisation in an area close to the subject. Placements are standard in all courses offered by the School of Computing and our experiences with them have been very encouraging. They allow students to apply their theoretical knowledge and expose them to the organizational environment in which most of them will eventually go to work. The third year placement within a forensic computing environment is important from the recruitment point of view since employers prefer recruits with practical experience (Janes, 2005). While placements are spent in an organisational environment, they are still supervised by academics and students' have to write an assignment in order to get their placement recognized. During their final year, students are required to undertake a major project, which can be directed towards research or the creation of a system. They have a choice of two smaller (15 credit) modules and have two more compulsory modules. The content of their modules will now be described in two sections technical/legal and professional/ethical.

The evaluation of the different modules will depend on their content. Traditionally, the technical modules that require hands-on activity are assessed by practical tests in labs. Modules that have a theoretical and practical content will usually have one-part coursework assessment and an exam paper at the end of the module. Other modules with a more theoretical content, such as the legal and professional modules, will require students to submit coursework, usually in the form of essays and presentations. This mix of different assessment modes will also help students develop a range of different skills and will thereby support the interdisciplinary education of the students.

One common source of tension in obtaining, presenting, and understanding technical evidence is the difference in mindset between the technical and normative worlds. If code works, background study and documented analysis is generally irrelevant. But lawyers depend increasingly upon the advance preparation of reports compulsorily required in the discovery process. Answers are useless unless the reasoning, background, and process are properly chronicled and legally obtained (Slade, 2004). From the outset students whose propensity is for either the technical or normative side of the course will be encouraged to work to see the other's point of view.

Technical Content

As can be seen from the appendix, half of the teaching time during the first two years will be allocated to purely technical topics. Students will in the first year learn the fundamentals of computer science as well as an introduction to programming in C. It was felt that, in order to be able to work successfully in forensic computing, students would need a broad general understanding of computing and ICT. This includes an understanding of modern programming as well as a general overview of hardware, software, and related concepts. These basic skills will be taught in the two first year modules, "Programming in C" and "Foundations of Computer Science". During the second year students will build on these foundations and be introduced to more advanced topics in the modules "Internet Software Development" and "Systems Programming".

For a student to become an effective investigator, it is our belief that they need to have spent some time approaching the technical material from a creative, rather than an analytical, point of view, in effect, creating digital evidence. These technical modules in the first two years therefore develop, albeit in a somewhat limited extent, the mindset of the conventional applied computer scientist. In particular, deep understanding of the way that data is stored on, or communicated between, computer systems is clearly critical to the ability to perform a digital investigation.

It was perceived that it would be useful to tailor the technical modules to the specific needs of forensic computing. Students might have been exposed to hardware and software tools used by the police force or they could have learned about issues of interest in criminal investigations such as encryption or specific technical platforms. However, for economic reasons it was considered to be impossible to create such new modules. If the number of students on the course becomes sufficiently large, the modules will be customized for the needs of the students.

In the final year, students have some choice regarding their specialization. They can choose further technical topics such as compilers and network protocols but they are also free to look in more depth at organizational or social issues such as privacy and data protection. Their final year project can also be of a technical or a research-oriented nature, depending on their interests.

Legal, Professional, and Ethical Content

As indicated earlier, our requirements analysis led us to believe that nontechnical skills are at least as important to forensic computing scientists as technical ones. We therefore dedicated the same amount of time to nontechnical issues that are specific to forensic computing. In the first year, this includes a module that describes the “Essentials of Forensic Investigations”. This module was developed for a forensic science course and includes the basic problems and questions of forensic science in a general way.

The final first year module, called “Normative Foundations of Forensic Computing” is divided into four main themes and will be delivered over the course of the year. The four main themes are,

1. **Ethical and moral questions in forensic computing:** This will provide students with an introduction to ethics and morality. They will be encouraged to understand morality as an expression of social preference/need and to recognize manifestations of this in several areas associated with computer forensics. These include intellectual property rights issues, privacy/ surveillance issues, access to data issues and issues of human-computer interaction. The theme will also provide an overview of ethical theories and explain these as reflections of morality. Building upon this, students will be encouraged to apply ethical reasoning to moral cases.
2. **Foundations of the law:** This theme will provide students with an essential understanding of what law is and with the ability to relate their understanding of it to forensic computing scenarios. The part played by ethics and morality in the

development of the law will be overviewed and students will be introduced to the common law, case law, and legislative sources. Probably one of the most important functions of this theme will be to equip students with the “know-how” to undertake research in legal issues relevant to forensic computing. This will be accomplished by careful *in situ* explanation of the law library so that students will be able to navigate and utilize its contents independently. Additionally, students will be familiarized with online sources of legal information. The theme will also be directed at elucidating legal language so that students can move confidently through legal texts.

Such skills are indispensable to a main aim of the module that of developing critical competence. Students will be asked to critically reflect, taking account of the current legal situation, on the role of forensic computing professionals and to discuss ethical and legal issues they may face.

3. **Substantive law in computing:** This theme will provide students with an understanding of the principles that the courts apply in their approach to cases involving computer crime. This will be accomplished by examining examples provided in case law and by scrutinizing the relevant legislation. Students will then be provided with hypothetical scenes of computer crime including evidential scenarios that they will be expected to relate to the relevant law and for which they will be expected to assess likely outcomes. Areas of computer crime to be studied include computer fraud, unauthorized access to computer materials, unauthorized modifications to computer data, piracy, and computer pornography and harassment. The theme will also cover instances where technology is involved in “traditional” crimes such as murder.
4. **Forensic issues in computer crime:** This theme will introduce students to the practical issues that arise in relation to forensic issues and computer crime. Students will be made aware of the importance of recognizing when in the course of their investigation they are about to take an action upon which legislation and case law impacts. The main areas to be covered in this part of the course are the search and seizure of evidence of computer crime, the interception of computer crime, and the preservation of evidence of computer crime. It will be necessary also to ensure that students are familiarized with the international approach to computer forensics.

The second year will be linked to the content of the first year. Students will attend a module on “Forensic Data Analysis” where specific forensic issues of databases will be taught. In parallel they will be taught “Issues in Criminal Justice”, to be delivered by the Law School, which will build on the legal knowledge they acquired in the first year.

The third year of the course will comprise students either in placements with the police or with a commercial organization. It is expected that the knowledge they will have gained in the first and second years of the course will have provided students with a sufficient level of understanding to be able to follow the daily routine of a forensic computing professional and, where it is appropriate, to work independently.

The fourth and final year of the course is designed to prepare the students for their emergence as qualified professionals in computer forensics. The two main modules, next to the final year project and the electives, are designed to simulate the environment in which the students will work after graduation. The “Digital Evidence” module will provide a number of case studies that will use real-life problems and data and show students the current tools, technologies, and techniques used by high-tech crime units. The design of this module, has of itself produced huge ethical challenges. How do we provide students with data to investigate which has been ethically obtained yet is sufficiently large in quantity and representative in quality to give them a realistic challenge? Similarly, do we explicitly teach students to hack systems so they can recognize the patterns of hacking? Further, how do we protect the University’s IT infrastructure from the various malevolent things (viruses or password cracking tools for example) that they will be studying? Substantial effort continues to be expended developing the tools, working practices, and physical and logical investigative environment so we provide safe educational experiences. Parallel to this, students will follow the module “Professionalism in Forensic Computing”. This module will build on the professional and ethical foundations of the first year module. It will continue to link the technical knowledge the student will have at this stage with their legal and professional experience. An important part of the module will consist of mock trials or “moots” where students will take the role of expert witnesses, for the prosecution or the defense, and where they will be asked to present evidence in the manner of policemen or expert witnesses in a court of law. The two modules will be closely related and the presentation of the evidence will be based on the technical case studies of the “Digital Evidence” module.

Problems of the Course

We hope that the above description of the rationale, requirements, and implementation of the forensic computing course will have convinced the reader that we have managed to create a viable, worthwhile, and interesting course. We should admit, however, that this set up contains several problems. Some of these are probably generic to all university courses, some specific to the university, while others would seem to be typical of interdisciplinary courses.

The general problems include questions of resources and economic viability. Ideally, we would have designed all new modules for the course but that would have required large student numbers, which we are not likely to obtain, at least not at the start of the course. Another general problem is the question of the limits that students need to know. It is always desirable for students (and anybody else, for that matter) to know more than they do. The technological knowledge could be extended to other technical platforms, such as handheld or mobile devices, to more than one programming language, to more software tools, and so on. Similarly, on the legal side, it would be desirable for students to have a good understanding of all legal matters related to forensic computing and maybe even be solicitors or barristers. There is thus the difficult problem of drawing the line between the knowledge that will be essential and that which they cannot be taught. A related

problem is that of the evolution of knowledge and the resulting fact that universities must teach students how to learn independently to keep up to date, rather than given them material knowledge that becomes outdated quickly. This is true for most subjects, and it is certainly true for something developing as quickly as information technology and its possible criminal applications. Our endeavour to ensure student competency in the handling of legal materials and familiarity with forensic tools, it is hoped, will go a considerable way towards assuaging this problem. Apart from such general problems that all university courses face, the interdisciplinary nature of forensic computing posed several unique challenges. The main problem is that the individuals who are knowledgeable in one field usually do not have expertise in the other fields. In our case, the two big groups of disciplines can be called the technical and the normative. The first includes all of the technical issues from hardware to software, networks, and so forth. The normative knowledge refers to the legal but also to the ethical and professional issues involved. While the individuals within the two groups may not always be aware of all the details in their own group (a hardware specialist may not be a specialist in programming; a legal scholar may not be an ethical expert), they are usually sufficiently similar in their knowledge and worldviews to be able to communicate. The same cannot be said for members of the different groups. Legal scholars do not have to be computer literate and an expert programmer may not have the first clue of the law. This is partly a result of the disciplinary division of academia and often produces no problems. This changes, however, when the different individuals need to agree on the set up of a course and when they have to collaborate to make it successful. For the nontechnical legal expert it is very difficult to assess the level of technical knowledge required to competently present digital evidence in a court of law. Similarly, the technical expert will find it hard to assess which legal or ethical constraints apply in their approach to possible evidence. To have it otherwise requires individuals who are experts in both fields and these are rare beings. They are also unlikely to be found in universities where, lip service withstanding, scholars are encouraged to stay within their disciplinary boundaries.

Another resource issue is that of the provision of specific equipment for such a course. Some of the modules can be taught in traditional labs which allow access for all our students. However, it is clear that the most interesting part of the course will necessitate specific equipment in the form of hardware, software, and regulations, which will only be accessible to students of the course. Examples are viruses and worms and other malicious software that students have to learn to deal with. They will furthermore be required to undertake actions, albeit under strict supervision, that will normally be prohibited for students. They will learn to tinker with security mechanisms and to access data that users don't want to access. These considerations led the management of the school to the decision to create a new laboratory which is to be used exclusively by forensic computing students and staff.

A final set of problems has to do with the question of critical reflection and the role of forensic computing professionals in society. The above outline of the course shows that our students will be quite busy learning the material presented to them. Critical reflection, which universities tend to see as a desirable skill to be taught to students, can easily be forgotten in the rush. Or, if it is actually addressed, it may be applied to limited areas, such as in a critique of certain tools or legal precedents. This is problematic because the work of a forensic computing professional is likely to involve activities which are located at

some of the major fault-lines of societal discourses. It will have to do with fundamental ethical and social issues. Obvious examples are issues of privacy or intellectual property. Businesses who employ our graduates are likely to use employee surveillance and the graduates' skills will be well-suited to the identification of employees who misuse company equipment for personal purposes. At the same time, one must be aware that the very idea of employee surveillance is highly contentious (Stahl, Prior, Wilford, & Collins, 2005) and that the role of the computing expert is anything but neutral. A similar case can also be made regarding possible uses of the students' skills in public service in the police force. Forensic computing can be used to identify the illegal use or duplication of copyright material. There have been a number of high profile court cases in the last few years in which major holders of intellectual property (music labels, film studios, software companies) have controversially asserted their rights by suing individuals. The very issue of intellectual property is contested (Stahl, 2005) and the forensic computing scientist needs to be aware of the influence he or she may have on social debates. Clearly there is great scope for critical reflection upon the role of forensic computing in society. It is highly desirable that students be capable of taking a coherent stance on these matters and that they are able to defend it, but it is open to debate whether students will in fact have the time or be prepared to undertake critical analysis sufficient for the consideration of other stakeholders' views.

Conclusion

This paper set out to describe the challenges encountered by the School of Computing of De Montfort University in establishing a course in forensic computing. The course is due to start in the autumn of 2005, given that a sufficient number of students enrol. This paper is more a reflective account of the creation of the course than a classical academic paper. We hope nevertheless that it will be of interest to the audience of the book because it highlights some of the problems that will have to be addressed if forensic computing is to become a recognized profession. The paper has given an authentic account of the history and intended structure of the course. It has also outlined some of the problems we have had and that we foresee for the future. We do not claim to have found all the right answers. Instead, we hope that the paper will work as a basis of discussion for people and institutions with similar questions.

References

- Block, W. (2001). Cyberslacking, business ethics and managerial economics. *Journal of Business Ethics*, 33, 225–231.
- Deats, M. (2005, April 28). Quoted by Clint Witchalls in Digital Detectives. *The Guardian*, 19.
- Janes, S. (2005, April 28) Quoted by Clint Withcalls in *The Guardian*, 19.

- Slade, R. (2004). *Software forensics*. McGraw Hill. 87.
- Stahl, B. (2005). The impact of open source development on the social construction of intellectual property. In S. Koch (Ed.), *Free/Open Source Software Development* (pp. 259-272). Hershey, PA: Idea Group Publishing.
- Stahl, B., Prior, M., Wilford, S., & Collins, D. (2005). Electronic monitoring in the workplace: If people don't care, then what is the relevance? In J. Weckert (Ed.), *Electronic Monitoring in the Workplace: Controversies and Solutions* (pp. 50-78). Hershey, PA: Idea-Group Publishing.
- Straub, D. & Collins, R. (1990). Key information liability issues facing managers: Software piracy, proprietary databases, and individual rights to privacy. *MIS Quarterly*, 14, 143-156.
- Tapia, A. (2004). Resistance of deviance? A high-tech workplace during the bursting of the dot-com bubble. In B. Kaplan, D. Truex, D. Wastell, A. Wood-Harper, & J. DeGross (Eds.), *Information Systems Research: Relevant Theory and Informed Practice* (pp. 577-596) (IFIP 8.2 Proceedings). Dordrecht: Kluwer.
- Tavani, H. (2001). Defining the boundaries of computer crime: Piracy, break-ins, and sabotage in cyberspace. In R. Spinello, & H. Tavani (Eds.), *Readings in Cyberethics* (pp. 451-462). Sudbury, Massachusetts: Jones and Bartlett.
- Urbaczewski, A., & Jessup, L. (2002). Does electronic monitoring of employee internet usage work? *Communications of the ACM*, 45(1), 80-83.
- Witchalls, C. (2005, April 28). Digital detectives. *The Guardian*.

Appendix A: Draft Course Structure of the BSc Forensic Computing

Year 1	CSCI1401 Programming in C (30 credit) Existing module	CSCI1408 Foundations of Computer Science (30 credit) Existing module	CHEM1050 Essentials of Forensic Investigations (30 credit) Existing module from Applied Sciences	INFO1412 Normative Foundations of Forensic Computing (30 credit) New Module <i>Establishes the ethical and regulatory framework within which an investigator must operate</i>	
Year 2	CSCI2404 Internet Software Development (30 credit) Existing module	CSCI2410 Systems Programming (30 credit) Existing module	INFO2425 Forensic Data Analysis (30 credit) New Module <i>But built from the 15 credit module that rgh delivers to BSc Forensic Science – needs some database content</i>	LAWG2003 Issues in Criminal Justice (30 credit) Existing module from Law Dept	
Placement year					
Year 4	CPRJ3451 Computing Double project (30 credit) Existing module	Option 1 (15 credit) Existing module	Option 2 (15 credit) Existing module	CSCI3427 Digital Evidence (30 credit) New module <i>Series of case studies, using tools and techniques to detect, preserve, analyse and present digital evidence from a variety of devices.</i>	INFO3427 Professionalism in Forensic Computing (30 credit) New module

BSc Hons Forensic Computing – Draft Course Structure - I

Example final year options include:

CSCI3401 – Broadband Networks

CSCI3402 – Network Protocols

CSCI3405 – Genetic Algorithms and Artificial Neural Networks

CSCI3406 – Fuzzy Logic and Knowledge-based Systems

CSCI3412 – Compilers

CSCI3426 – Telematics

INFO3406 – Privacy and Data protection

INFO3421 – Database Management Systems

Appendix B: Syllabi of New Modules to be Developed for the Course

Appendix B1: Normative Foundations of Forensic Computing

1. Ethical and moral questions in forensic computing

- Introduction to ethics and morality
- Morality as an expression of social preferences
- Examples of moral problems in computing
 - intellectual property
 - privacy / surveillance
 - access
 - human - computer interaction
 - ...
- Ethics as the theoretical reflection of morality
- An overview of ethical theory
 - classical Greek ethics
 - virtue ethics
 - deontology
 - teleology
 - ethical scepticism
 - modern approaches to ethics
 - ...
- Application of ethical reasoning to moral cases
- Reading and understanding ethical texts

2. Foundation of the law

- Historical development of legal systems
- ethics, morality, and the law
- sources of law (civil law, case law traditions, influence of the EU on UK law)
- understanding legal language
- doing research in legal issues

3. Substantive Law in Computing

- Introduction to computer crime
- Computer fraud
- Hacking— unauthorised access to computer materials
- Unauthorised modifications to computer data
- Piracy and related offences
- Computer pornography and harassment

4. Procedural Law in Forensic Computing

- Introduction to forensic issues and computer crime
- The search and seizure of evidence of computer crime
- The interception of evidence of computer crime
- The preservation of evidence of computer crime
- International harmonization and assistance in computer forensics
- Review of legislative issues in computer forensics

B2: Forensic Data Analysis

The following represents a broad range of topics that can be addressed within this module. The actual emphasis and topics covered each year will depend on the availability of expert speakers and changes in the subject.

Indicative Content:

Intro to Module: content & assessment

Introduction to Literature Review, Writing Academic Papers and Presenting the Results

Intro to Forensic Data Analysis

Role of data and data management in Forensic IT

Data analysis, normalisation and determinacy

Database design, implementation, interrogation and management

Using databases to facilitate forensic investigations

Forensic Computing and Forensic Data Analysis

The use of IT in criminal activities

- E-crime
- E-terrorism
- Credit card fraud
- Internet abuse

Computer Security

Incident response—preserving forensic data as admissible evidence; strategies, techniques and challenges

Incident response strategies for specific types of cases

Data hiding strategies

Data discovery and analysis strategies

Email investigations and data analysis

Image file investigations and data analysis

Forensic Software, FRED and other data analysis software

Use of data in the judicial system

Modern and developing forensic data analysis technologies, ie:

- Image analysis, enhancement and facial reconstruction
- DNA databases, human genome project and fingerprint comparison
- AI and forensic data analysis

B3: Digital Evidence

Tools

- low-level tools to examine blocks on disks, partition tables, file dumps, network packets etc.
- specific tools for particular tasks / device types,
- tool capabilities and limitations,
- specialist forensic toolsets (such as EnCase).

Working Practice

- ACPO Good Practice Guide for Computer based Electronic Evidence.
- RIPA— Regulation and Investigatory Powers Act,
- Maintenance of evidence audit trail.

Detection

- security (logging, port monitoring, traffic monitoring),

Preservation

- data volatility— order of volatility— order of recovery,
- duplication (bit copy) of original data to two locations prior to analysis,
- verification of copy via hash value(s),
- Hard Disc Drive / boot disc preservation

Analysis

- Reconstructing fragments of data,
- determining significance,
- drawing conclusions based on evidence,
- hypothesis generation and confirmation.

Presentation (*it is probable that this aspect will operate in conjunction with INFO3427*)

- audience, assumptions about prior knowledge, especially expert vs lay person,
- technical report
- oral cross examination such as would be expected in court

B4: Professionalism in Forensic Computing

1. Framework of Professionalism in Forensic Computing (1st half)

- Introduction to legal philosophy (positivism vs. conventionalism)
- Ethics and Human Rights
- Critical Analysis of the role of law enforcement and its agents in society.

2. Professional Conduct in Forensic Computing (1st half)

- Code of Conduct for police officers
- Ethical reflection of this code of conduct
- Stakeholder analysis in investigative work
- Discussion of conflicts of interest
- Application to case studies
- The first half of the module (semester 1) will be assessed through an essay.

3. Professional Presentation of Evidence (2nd half)

- Gathering evidence
- Legal interpretation and presentation of technical evidence
- Court room presentation scenarios (moot)
- This module will be closely related to the Digital Evidence module in order to develop the technical skills acquired there for use in the preparation and presentation of evidence.
- The module will involve “real life” preparation and presentation of evidence and will be conducted in close collaboration with the police.
- This half of the module will be marked through examination of the skills displayed during the court room presentation scenario (moot).

Endnotes

- ⁱ We should clarify at this stage what we mean by “course”. A university course in the UK stands for the totality of teaching that a student is exposed to in order to receive a degree. It is thus what might be called a “program” in the US and elsewhere. A single unit in such a course, which typically lasts a semester, or a year in the case of DMU, is called a module.
- ⁱⁱ According to Simon Janes international operations director for the computer security firm Ibis less than 1% of the UK police force is trained to gather computer evidence and there are estimated to be less than 100 experts in the UK capable of analyzing computer evidence to the standard of the court. Janes was interviewed by Clint Witchalls for an article entitled “Digital Detectives”, *The Guardian*, April 28th, 2005, page 19.
- ⁱⁱⁱ Botnets consist of thousands of compromised computers working together. The combined processing power is harnessed in a “herding” process and used to send massive quantities of spam or to carry out denial of service attacks.