# An Interdisciplinary Approach to Forensic IT and Forensic Psychology Education

Clare Wilson[1], Vasilios Katos[2], Caroline Strevens[3]

[1] Department of Psychology, University of Portsmouth, UK
[2] School of Computing, University of Portsmouth, UK
[3] Department of Accounting and Law, University of Portsmouth, UK
{clare.wilson, vasilios.katos, caroline.strevens}@port.ac.uk

**Abstract.** In WISE 4, Armstrong [1] presented a multidisciplinary view in computer forensics education. The view was primarily focusing solely on the education of computer forensics students, which was indeed along the lines of multidisciplinarity. However, this view does not involve integration between the different disciplines. In this paper, the scope of the approach is extended in order to allow a two- or three-way relationship between the disciplines of Computing, Psychology and Law and thus create an interdisciplinary perspective. It is shown how the study material was integrated and developed to suit the three disciplines.

**Keywords:** computer forensics, forensic psychology, expert testimony.

## 1 Introduction

Both multidisciplinarity and interdisciplinarity have received in recent years a significant amount of attention not only in the area of security education, but in a variety of fields. For example, Browne [2] discusses the impact of an interdisciplinary approach to environmental education and Gardner *et al.* [3] address the relevant needs in healthcare. With respect to security education, Gritzalis *et al.* [4] present a detailed analysis towards developing an interdisciplinary model for information security education.

It is argued that a multidisciplinary approach is not sufficient in forensic education, due to the nature of forensics. The main reason is that forensic science is in its minimum a bi-disciplinary subject, encompassing a scientific component and a legal component. Yasinsac *et al.* [5] categorically identify that a computer forensic scientist must have a background in Computer Science, Law and Forensics. Furthermore, the forensic analysis process operates in an open and complex problem space, due to the increased uncertainty. If for instance a forensic investigation refers to an activity attributed to an individual or a group of people, psychology would play an important role.

Interdisciplinarity on the other hand refers to the integration of different perspectives into an epistemological identity [4]. For a forensic investigator, learning to manage and work across many disciplines is indeed a critical success factor. This

*Please use the following format when citing this chapter:*

Wilson, C., Katos, V., Stevens, C., 2007, in IFIP International Federation for Information Processing, Volume 237, Fifth World Conference on Information Security Education, eds. Futcher, L., Dodge, R., (Boston: Springer), pp. 65–71.

can be easily established if the forensic investigation is viewed as a research process; in research, many of the intellectual breakthroughs were made by crossing disciplinary boundaries [6]. An explanation to Morillo's et al. statement can be found in Barker *et al.* [7], who reason that researchers make valuable contributions to fields outside of their specialty by asking questions from a different viewpoint, as opposed to the narrower perspective of the "insiders" of the field.

The above setting is prevalent in computer forensics. For example, a suspect hard disk may host encrypted data and the path to decrypting the data (assuming that all cryptanalytic attacks have failed and the only option left is exhaustive search) is usually to construct a case specific dictionary, to mount a dictionary attack. The psychology of the suspect may aid the investigation, for example, offender profiling may indicate certain tastes and preferences in the suspect which may help in constructing a candidate list of passwords. Similarly, information obtained from the analysis of the digital evidence may contribute to the understanding of the socio-psychological behaviour of the suspect.

The rest of this paper is structured as follows. In Section 2 there is a brief discussion of the MSc programmes in Forensic IT and Forensic Psychology taught at the University of Portsmouth. Section 3 describes the forensic process exercise, as it spawns between the two disciplines and concludes with the mock trial involving the law students from the Department of Accounting and Law. Section 4 presents lessons learned and areas for further development.

## 2 Forensic IT and Forensic Psychology

The structure of the MSc in Forensic IT is depicted in Fig. 1. Albeit exhibiting a modular approach, all modules are stemming from the "Digital Forensics" module. More precisely, the process of acquisition, preservation, analysis and reporting is covered by the digital forensics unit, but the more advanced skills required to perform the individual processes are covered by the supporting modules of cryptography, offender profiling, network security, data mining, white collar crime, cyber crime and strategic risk management.

The MSc in Forensic Psychology is also a modular design, all integrated to examine the criminal behaviour, investigation, prosecution and treatment of offenders. One module, Psychology and Investigations, was dedicated to the examination of the same case module used in the Digital Forensics module of the MSc in Forensic IT.

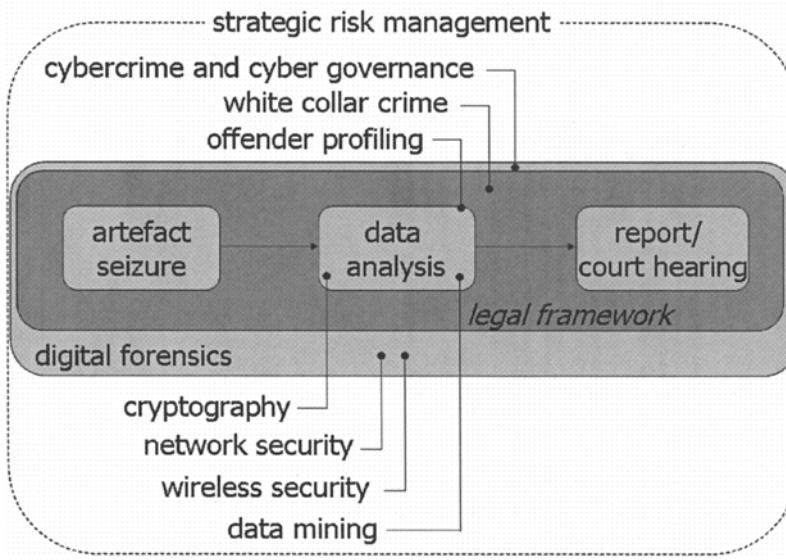


**Fig. 1.** The MSc in Forensic IT structure

### 2.1 The digital forensics laboratory

The Digital Forensics Lab (DFL) is a specialised, state of the art laboratory, enabling the students undertaking the digital forensics and network security module (which primarily focuses on the network forensics aspects), to gain practical, hands on experience on forensic discovery of digital storage media.

The DFL is equipped with both open source and commercial software and specialist hardware (such as hardware blockers, hardware bitstream copying devices). The lab consists of three rooms: the main teaching room, the evidence room which contains lockable cabinets where the students are assigned keys for accessing the evidence, and the production room which hosts the servers and network equipment.

The lab is self sustained, with two networks, namely the attack network and the forensic network. The former is used for studying network security related issues, such as denial of service attacks, vulnerability scanning, code injection etc. It is envisaged that in the longer run it will be able to regularly participate in cyber security exercises (see for example Dodge *et al.* [8]). The latter network allows limited access to the internet, which is needed in order to complete certain tasks.

Students use the lab to study digital forensics, cryptography and network security. Due to the nature of the course, the forensic students have exclusive access to the lab and are required to subscribe to a code of ethics. The lab complies with certain requirements relating to forensic investigations (swipe card access, no windows, and no false ceilings). Furthermore, the students have limited technical support and in effect have the "ownership" of the lab; they have administrative access to the

computers and they are responsible for the maintenance of the equipment. This is required as it is a vital component of the adopted teaching and learning strategy and furthermore this responsibility is part of the skills they need to acquire in order to be prepared to face real life scenarios once they graduate from the course.

## 3 The Module Delivery Process

The case study was jointly developed by the Department of Psychology and the School of Computing of the University of Portsmouth.

The case involved the alleged rape and murder of a student, Ms Ima Meanie (a woman with Dissociative Identity Disorder) by a computer technician, Mr Gil T. Ornot. A depressed student associate of Ms Meanie, Ms Clare-Lee Blue also alleged rape by Mr Ornot. However, Mr Ornot's flatmate, Ali Bye, maintained that Mr Ornot was with him the whole time. However, computer files of the case can disprove statements made by Mr Ornot and Mr Bye.

A disk image was developed reflecting aspects of the chronology of events. The key digital evidence was a collection of photographs, chat logs and an encrypted volume. The latter was a bad extension file, where the students were required to examine the file header to establish the correct file type and proceed with recovering the evidence.

The digital investigation process was initiated by a search warrant (Fig. 2), requiring the students to form a team led by a nominated team member. Prior activities, apart from the technical training on forensic tools such as the Forensic Tool Kit and The Sleuth Kit with its front end (Autopsy), included the development of the relevant evidence forms, such as a Chain of Custody form and a Multi Evidence Form, as well as a documented, formal description of the evidence seizure process.

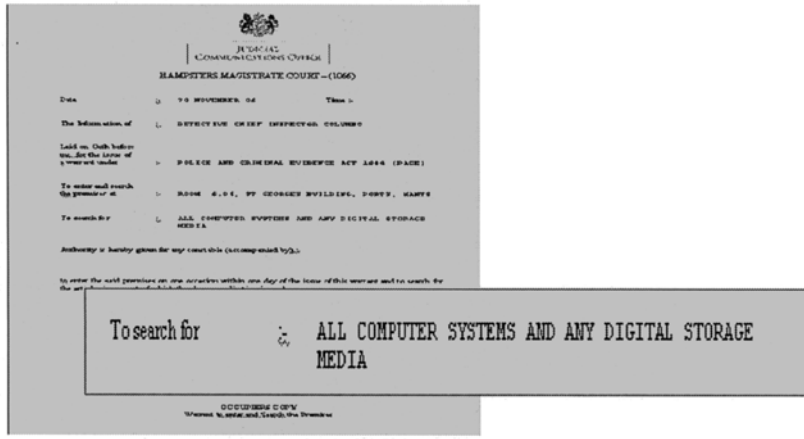


**Fig. 2.** The search warrant

The digital forensics team was equipped with the following equipment to handle the evidence discovered at the crime scene:

- cameras
- laptops with hardware write blockers
- evidence bags
- hardware forensic bit stream copying devices, capable of computing the MD5 and SHA-1 hashes of the acquired hard disks.

During the seizure all team members had clear roles and responsibilities assigned by the leader. The role allocation was performed prior to visiting the crime scene, as there was a briefing from the leader. The role allocation process considered the four Association of Chief Police Officers (ACPO) principles [9] and therefore the individual's expertise was taken into account.

Interdisciplinarity is further enforced with a formal meeting between the forensic psychologists and the computer forensics investigators, to exchange discovered information and consolidate findings. The psychologists were particularly interested in the timestamps of the digital files, in order to verify the chronology of events and establish whether the suspect lied during their testify statement. The forensic investigators were interested in understanding the personality attributes of the suspect, in order to narrow down the cryptanalytic attack to the encrypted files. The fact alone that certain files may be encrypted, as well as the type of the encrypted content in turn provided valuable information both to the psychologists and lawyers.

### 3.1. The path to court

In a criminal trial it is for the jury to decide on the facts proven. However they can be helped in this task with expert evidence. An expert is entitled to give an opinion only on relevant matters which are within his particular area of expertise and which are outside the general knowledge and understanding of the jury.

"[O]ne purpose of jury trials is to bring into the jury box a body of men and women who are able to judge ordinary day-to-day questions by their own standards, ... Where the matters in issue go outside that experience and they are invited to deal with someone supposedly abnormal, for example, supposedly suffering from insanity or diminished responsibility, then plainly in such a case they are entitled to the benefit of expert evidence." (R v Chard (1971) 56 Cr App R 268 (CA) pp 270 -1)

It was confirmed in R v Mackenney (No.2) 2004 2 Cr App R 32 that expert evidence is admissible on the reliability of the accused or some other witness testimony only if the evidence suggests a medical abnormality. Otherwise it is not admissible.

In the Crown court the judge, at the plea and case management hearing will make directions about whether expert evidence is to be obtained and if so what. The prosecution must serve expert testimony in report form on the defence before the trial starts. The defence must respond by submitting a Defence Case Statement setting out the general nature of the defence and what differences there are with the prosecution.

If the accused intends to rely on an alibi, further details must be served on the prosecution to enable them to bring evidence to refute this.

Thus it is apparent that the lawyers involved must be briefed on the technical aspects of expert testimony before they can advise on its admissibility or on the steps necessary to challenge it. In the case study it was decided only to involve the law students in the delivery of the evidence at trial rather than in its preparation and exchange (although it is planned to do so in subsequent academic years in conjunction with the delivery of a Law of Evidence module on the Legum Baccalaureus (LLB) or Batchelor of Law degree). In the case study law students were paired with psychology and forensics students in order for that briefing before the trial was to take place. The law students had to understand the technical issues in order to formulate the outcomes for the cross-examination and to prepare their questions.

An expert must be skilled in matters about which he is asked to give an opinion. He has an over-riding duty to help the court on the matter which overrides any obligation to the party from whom he received instructions. The expert must thus state his qualifications and experience in his evidence and will be open to cross-examination on this point. The expert must state in his report the main points of all written instructions given to him. This is in order to prevent the parties from asking the expert to change his conclusion. Any discrepancies will also be an area for cross-examination.

Although it is ultimately for the jury to decide the expert may give his opinion on the likely innocence or guilt of the accused.

The forensics students presented evidence as to the contents of the hard drive of the accused. They had to brief the law students on the authenticity of the materials found, and explain how any deleted files were recovered in secure form so that they could give evidence that there was no possibility of tampering by another person after the computer was seized.

## 4 Conclusions

In this paper an interdisciplinary approach for developing and delivering educational material for teaching forensic computing students and forensic psychologists, with the view of involving law students was presented.

The forensic students, both in psychology and computing, developed an appreciation for their peer forensic investigators and understood that integrating two disciplines on an epistemological level not only results in added value from an educational perspective, but also that it is of a paramount importance that forensic discovery involves different specialists in order to compensate for the significant uncertainty that governs the forensic analysis process.

The law students gained a valuable opportunity to learn a little more about the criminal justice process (outside the curriculum at undergraduate level – normally learned on a Legal Practice Course, LPC or a Bar Vocational Course, BVC) and to

hone their communication and advocacy skills. Although law students are used to Mooting, which involves presenting arguments on points of law, they do not often gain the experience of cross-examination.

## References


1. Armstrong, C., 2005, Computer Forensics Education – A Multi-Discipline View, WISE 4 Proceedings, Moscow, 18-20 May, pp.205-212.
2. Browne, M., 2002, The Mandate for Interdisciplinarity in Science Education: The Case of Economic and Environmental Sciences, Science & Education, 11, pp.513-522.
3. Gardner, S. Chamberlin, G., Heestad, D., Stowe, C., 2002, Interdisciplinary Didactic Instruction at Academic Health Centers in the United States: Attitudes and Barriers. Advances in Health Sciences Education, 7, pp. 179-190.
4. Gritzalis, D., Theoharidou, M., Kalimeri, E. 2005, Towards an Interdisciplinary Information Security Education Model., WISE 4 Proceedings, Moscow, 18-20 May, pp.22-35.
5. Yasinsac, A., Erbacjer, F., Marks, G., Pollitt, M., Sommer, M., 2003, Computer Forensics Education, IEEE Security and Privacy, 1(4) pp. 15-23.
6. Morillo, F., Bordons, M., Gomez, I., 2003, Interdisciplinarity in Science: A Tentative Typology of Disciplines and Research Areas, Journal of the Americal Society for Information Science and Technology, 54(13), pp.1237-1249.
7. Barker, R., Gilbreath, G., Stone, W. 1998, The Interdisciplinary needs of Organisations: Are New Employees Adequately Equipped?, Journal of Management Development, 17(3), pp.219-232.
8. Dodge, R., Hoffman, L., Ragsdale, D., Rosenberg, T., 2005, Exploring a Cyber Security Exercise, WISE 4 Proceedings, Moscow, 18-20 May, pp.94-101.
9. Association of Chief Police Officers (ACPO), Good Practice Guide for Computer based Electronic Evidence, National High Tech Crime Unit. Available at: http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf