

Development of masters modules in computer forensics and cybercrime for computer science and forensic science students

Richard E. Overill

Department of Computer Science,
King's College London,
Strand, London WC2R 2LS, UK
E-mail: richard.overill@kcl.ac.uk

Abstract: In mid-2004, it was decided that the list of optional modules available to students taking the MSc programme in Computing, Internet Law and Management at King's College London (KCL) should be supplemented with a module in computer forensics (CF) and cybercrime. It was proposed that this module should be delivered as a reading course to be assessed by means of a dissertation and a linked *viva voce* examination. We trace the evolution of this module over the three academic years from 2005/2006 to 2007/2008 inclusive and discuss the range of dissertation topics selected by the students. The results and the evidence from anonymous student feedback surveys are analysed quantitatively and are compared with those from a longer established module on forensic computing and CF which forms an integral part of the interdisciplinary MSc in Forensic Science at KCL. We conclude with a critical assessment of the success of both modules.

Keywords: CF; computer forensics; computer science; cybercrime; forensic science; MSc modules.

Reference to this paper should be made as follows: Overill R.E. (2009) 'Development of masters modules in computer forensics and cybercrime for computer science and forensic science students', *Int. J. Electronic Security and Digital Forensics*, Vol. 2, No. 2, pp.132–140.

Biographical note: Richard E. Overill is a Senior Lecturer in Computer Science at King's College London. His principal research interests currently lie in the field of information assurance and include anomaly detection, cyberforensics, information security management system (ISMS) architectures and analysis of cybercrime statistics.

1 Introduction and background

The MSc programme in Computing, Internet Law and Management (CILM) is one of four MSc programmes in Computer Science currently offered by King's College London (KCL) and it is the only one that can be taken in either full- or part-time modes of study. Teaching of the Internet Law and Management components has until now been subcontracted to the School of Law and the Department of Management, respectively. In mid-2004, it was decided to enhance the portfolio of optional computing modules on

offer to the MSc CILM students by the addition of a module entitled computer forensics and cybercrime, CSMCFC (2008a).

The stated aim of the module is “to provide students with a solid foundation to understand the concepts involved in both computer forensics and cybercrime”. Its learning outcomes are defined as follows:

“At the end of this module a student is expected to understand computer crime, together with its social and legal implications; understand the techniques for computer and network forensics; understand, and relate the above points to, the UK Computer Misuse Act and related EU legislation”, CSMCFC (2008b).

A significant feature of this module is that it is not delivered as a formally examined lecture course or as a laboratory-based course. Rather, it was decided that it should be offered as a reading course to be assessed by means of a written dissertation and an accompanying oral presentation to the assessors. This would also bring the MSc CILM into line with the other three full-time MSc programmes for which a dissertation-based optional module entitled Advanced Research Topics (code: CSMART) was already available.

In the following sections, we discuss the range of dissertation topics selected by the students, we analyse quantitatively the results obtained by the students over the past three successive academic years, and we evaluate the anonymous student feedback obtained via the standard KCL module evaluation MCQ. We conclude this paper with a critical assessment of the degree to which the published aims and objectives of the module have been successfully achieved, and some comparisons with the results of our previous studies in this area.

2 Dissertation topics

Students are free to select any dissertation topic in consultation with the module leader whose main functions are to ensure

- 1 that each topic selected clearly falls within the scope of the module
- 2 that the topic does not overlap significantly with those topics already selected by other students.

The topic selection process is preceded by an induction meeting at which the module leader outlines the scope of the module, indicates the principal resources available for research and explains how the dissertation and presentation are to be assessed. The list of dissertation topics selected by the students over the past three years is shown below; the four topics that were selected more than once in different academic years are marked (2): one topic was ultimately ruled out-of-scope:

- computer-related crime: hackers, malware and spyware
- computer-assisted crime: financial fraud, embezzlement and blackmail
- social engineering and cognitive hacking
- cyber-squatting (2)
- trojan horses (2)

- phishing attacks
- commercial espionage and sabotage
- biometrics: fingerprint analysis
- DNA cryptography
- digital IPR and music piracy
- cyber-stalking (2)
- antiforensics
- virtual crime
- cognitive hacking pump-and-dump schemes
- computer virtualisation in forensic investigations
- scams by cyber-criminals
- motivation of malware creators (2)
- virtual crime
- trends in cyber-warfare and national security in the internet age
- e-banking fraud.

While only two of the above topics are explicitly concerned with cyber-forensics *per se*, the remainder is implicitly linked to it *via* the traces that may be left at the scene-of-crime. The apparent imbalance in topic selection reflects the profile of the student intake to the MSc CILM programme where the part-time students almost without exception held full-time information security management posts and many of the full-time students held bachelors degrees with a strong law or management component. Only those full-time students holding single honours Computer Science BSc would be likely to consider the possibility of selecting a dissertation topic explicitly concerned with cyber-forensics.

3 Syllabus topics

It is instructive to compare the chosen dissertation topics above with the current syllabus topics for the forensic computing (FC) and computer forensics (CF) module of the MSc in Forensic Science at KCL, for which the author is also responsible. This may be summarised as follows.

Forensic computing:

- crime scene reconstruction, specifically the immersive environment Hydra system of the Metropolitan Police service
- blood spatter analysis, specifically the Delft Forensics Visual Sensor Fusion 3D Blood Pattern Analysis module

- facial reconstruction, specifically the 3D graphics systems by Robin Richards and Peter Vanezis
- computation and matching of biometrics, specifically fingerprints and iris scans using NAFIS and IrisCode, respectively
- construction and matching of offender profiles, specifically the FBI's VICAP system and the Home Office CATCHEM system.

Computer forensics:

- scoping and freezing the crime scene
- bit-wise imaging of all memory devices
- searching for unerased data in temporary files, swap space, spool areas, slack space, etc., specifically the use of an EnCase Forensic demonstrator (EnCase, 2008)
- scanning for the presence of Trojans, remote administration tools, root-kits, back-doors, etc.
- checking system logs/audit trails for evidence of malfeasance
- performing internet trace-backs via ISP log-files
- performing cyber-profiling
- legal issues, specifically the UK Computer Misuse Act (CMA, 1990) as modified by the Police and Justice Act (PJA, 2006).

These syllabus topics form the basis of the optional examination question that is set each year as part of the formal assessment of the MSc in Forensic Science.

4 Traditional forensics and CF

An important issue to be addressed is the interrelationship between CF and traditional forensic science topics. CF, in common with forensic science, adheres to the forensic principles of securing the crime scene, gathering, preserving and analysing the evidence and (if required) presenting the evidence in a court of law as an expert witness. Thus, students of forensic science can be expected to be familiar with the concepts of 'bag-and-tag', chain of custody, admissible evidence, etc. The forensic process is predicated upon Locard's exchange principle, first enunciated by Edmond Locard, which is usually summarised as 'every contact involves an exchange of material' or 'every contact leaves a trace' (Locard, 1910). In the case of traditional forensic science the physical exchange process may occur at the atomic, molecular, cellular or macroscopic sample level and its detection is achieved by performing specific analytical physicochemical tests. With cyber-forensics, on the other hand, when the internal state of a digital computer or network is altered by the intervention of an unauthorised agent, be it human, software or hardware, the mathematical-logical tests required to detect and interpret this state change are of an entirely different category.

An important question for discussion with forensic science students is whether Locard's exchange principle applies strictly in cyberspace – or, conversely, does a cybercrime potentially constitute 'the perfect crime'? A second issue that frequently arises from such discussions is precisely what constitutes the suspected cybercrime scene, particularly if, as is commonly the case, the computer system or network under investigation is (either directly or indirectly) connected to the internet? Springing directly from this consideration is a third issue relating to freezing the cybercrime scene. It is apparent that quite different procedures must be adopted to preserve evidence at a cybercrime scene where

- 1 a computer is found unattended and powered-off
- 2 the computer is unattended but powered-on and possibly online
- 3 the computer is attended, powered-on and possibly online.

Scenario (1) most closely resembles the crime scene of traditional forensic science, while scenario (2) requires an assessment of the potential for information loss as a result of either abruptly disconnecting the power supply or alternatively shutting down the computer. Scenario (3) leads naturally to a discussion of hot-key data erasure, and thence to the number of data erasure passes required to yield an insignificant probability of data recovery (Gutmann, 1996).

Another area of similarity between CF and traditional forensic science is that of offender profiling. It has been long been recognised that serial criminals tend to develop an individual *modus operandi* (MO) which can be used to identify and distinguish their crimes from evidence gathered at the crime scenes. However Clifford Stoll's use of a simple form of behavioural profiling in 1986 marked the first attempt to apply these principles to the activities of a cybercriminal (Markus Hess *aka* Jaeger) leading ultimately to his arrest and conviction (Stoll, 1988, 1990). Cyber-profiling has subsequently evolved into a relatively sophisticated discipline comparable with traditional offender profiling, as judged by the number of distinct behavioural attributes that are taken into consideration. Typical useful metrics include the following:

- what files/directories/databases are searched
- what keywords/key-phrases are searched for
- how frequently email/other users' activity is monitored
- the elapsed time of a typical online session
- the number of systems scanned
- the system/network scanning tools used
- what backdoors/Trojans/root-kits are exploited.

5 Analysis of results

The dissertation assessment scheme can be summarised as follows: A thorough literature review covering the whole topic is normally awarded a Pass. In addition, a rigorous critical analysis, assessment and evaluation of the selected topic are normally awarded Merit. Further, an original proposal or novel contribution to the selected topic is normally

awarded Distinction. The recommended dissertation length is 3,000 words. All student dissertations were independently double marked and the individual marks were then reconciled and ranked by three assessors working as a team. Turnitin and Google were routinely employed to look for evidence of direct plagiarism in all the dissertations; the students were prewarned of this. Where a topic had been selected previously the electronic copy of the previous dissertation was also checked. The results are displayed in the table follows (Pass = 50+; Merit = 60+; Distinction = 70+):

<i>AY</i>	<i>#Stdis.</i>	<i>#F/T</i>	<i>#P/T</i>	<i>#Fail</i>	<i>#Pass</i>	<i>#Merit</i>	<i>#Dist</i>	<i>Mean</i>
2005/2006	3	0	3	0	3	0	0	58.0
2006/2007	12	10	2	1	5	4	2	57.1
2007/2008	10	10	0	1	4	4	1	59.8
Overall	25	20	5	2	12	8	3	58.3

While the year-on-year trend for average mark is essentially constant at a high Pass, the overall category profile reveals 12% Distinctions, 32% Merits, 48% Passes and 8% Fails. This shows that although the students self-selected their dissertation topics they nevertheless found it challenging to perform the task at an advanced Masters level.

By way of comparison, in the table below, we give the mean results of students opting to answer the examination question relating to the FC and CF module from the MSc in Forensic Science at KCL.

<i>AY</i>	<i>1995/1996</i>	<i>1996/1997</i>	<i>1997/1998</i>	<i>1998/1999</i>	<i>1999/2000</i>	<i>2000/2001</i>	<i>2001/2002</i>	<i>2002/2003</i>	<i>2003/2004</i>	<i>2004/2005</i>	<i>2005/2006</i>	<i>2006/2007</i>
#Ans.	17	14	9	11	32	0	3	3	6	6	6	6
FC/CF	FC	CF	CF	CF	CF	FC	CF	CF	FC	FC	CF	FC
Mean	48.5	40.3	52.2	60.9	48.3	–	56.0	59.8	45.3	52.0	64.5	48.2

A roughly equal balance was intentionally maintained between examination questions from the FC and the CF themes. The data appears to show that the students answered the CF questions with a slightly higher overall average (50.5%) than the FC questions (48.5%). However, care should be exercised in interpreting these data; the difference between the two averages are barely statistically significant.

6 Student feedback

The standard KCL module evaluation MCQ contains 12 positive statements about the delivery and content of the module to each of which all students taking the module are encouraged to respond with one of five responses ranging from strong disagreement, through undecided, to strong agreement. The students’ responses to the statements are gathered anonymously at the end of the module and then only if more than three students are taking the module. Students also have the option to append a freehand comment to the MCQ. In fact, four of the statements are inapplicable to a reading course and these were therefore removed from the MCQ. The results of the survey (in the form of percentages) are displayed in the following table:

<i>Statement</i>	<i>Strongly disagree</i>	<i>Disagree</i>	<i>Undecided</i>	<i>Agree</i>	<i>Strongly agree</i>
A	0	0	10	50	40
B	0	0	0	30	70
C	0	0	10	50	40
D	0	0	20	40	40
F	0	10	0	40	50
G	0	0	30	30	40
J	0	0	20	30	50
L	0	0	0	40	60

A standard measure of overall student satisfaction (MOSS) is to take the ratio of the number of responses in the agree/strongly agree categories to the total number of responses. In this case, we obtain a MOSS value of 0.875, which equates to a student satisfaction rating of 87.5% for the module. The sole freehand student comment on the module is perhaps worth quoting *verbatim*: “Great course. Dr Overill is friendly, knowledgeable and approachable. I was a little concerned at first about unclear requirements but the lecturer clarified. You get what you are willing to put into the course”.

The MOSS value above may be usefully compared with the aggregate student assessment scores for the past seven years from the FC and CF module of the MSc in Forensic Science at KCL, as shown in the following table:

<i>AY</i>	<i>2000/ 2001</i>	<i>2001/ 2002</i>	<i>2002/ 2003</i>	<i>2003/ 2004</i>	<i>2004/ 2005</i>	<i>2005/ 2006</i>	<i>2006/ 2007</i>
Std. scores	90%	79%	62%	65%	79%	80%	72%
#Stdts.	32	39	35	42	38	44	35

We note that there is a significant year-on-year variation in these scores. They are in fact derived from a somewhat different form of MCQ than those for the CSMCFC module above. However, it is possible to obtain an approximately comparable MOSS value by taking the weighted mean of the student assessment scores over the seven-year period. This yields a MOSS value of 75.1%, which is notably 12.4% lower than the MOSS value for CSMCFC. A possible explanation for this is that by no means all of the students in each MSc in Forensic Science cohort were convinced that CF forms an integral part of the discipline of Forensic Science and therefore tended to downgrade its significance.

7 Summary and conclusions

The results presented in this paper can be compared with those from two previous quantitative studies in which a CF-based curriculum is delivered to MSc students of Forensic Science and to MSc students of Computer Science (Overill, 2007; Overill and Ferguson, 2007). The average percentage marks (rounded to the nearest integer) for each of these four MSc programmes are collected together in the table below:

<i>Programme</i>	<i>Institution</i>	<i># Years data</i>	<i>Assessment</i>	<i>Average</i>
MSc For.Sci.	KCL	7	Examination	51
MSc For.Sci.	U. Strathclyde	4	Exam. + Lab.	55
MSc For.Inf.	U. Strathclyde	4	Exam. + Lab.	53
MSc CILM	KCL	3	Dissertation	58

The rather higher average mark for the dissertation-based mode of assessment is not entirely unexpected; conversely, the slightly lower average mark for the examination only mode of assessment is indicative of the influence of time pressure on the students' performance.

Perhaps somewhat surprisingly, the adoption of a reading course format for a Masters level module in CF and Cybercrime, assessed by means of a self-selected dissertation of 3,000 words and an accompanying oral presentation, has proved remarkably successful in fulfilling the stated aims and objectives of the module. This is due in some measure to the fact that the students are able to tailor the module to their own individual interests. To avoid the module becoming too narrowly focussed all students are expected to attend all the presentations. Students are also encouraged to visit the module leader for informal one-to-one on-demand mini-supervisions of about 30–60 min duration during the selection, planning and writing of their dissertations. It is noticeable that the students who make sensible use of this facility tend to be those who obtain the higher marks.

The module has recently been transferred into the core module set for the MSc CILM at KCL and is also designated a core module for the new MSc in Computing and Security commencing in 2008/2009. Finally, as a result of feedback from some students with a specific interest in cyber-forensics, it is planned to make a bid to the KCL Teaching Strategy Fund to establish a small cyber-forensics laboratory, in order to give such students the opportunity to gain some hands-on experience in this increasingly significant discipline.

A preliminary account of this study appeared in Overill (2008).

Acknowledgements

The author gratefully acknowledges Dr. Ian Ferguson (Department of Computer Science, University of Strathclyde) for the data taken from Overill & Ferguson (2008) and Prof. Terry Gough, Prof David Cowan and Dr. Barbara Daniel (Department of Forensic Science and Drug Monitoring, King's College London) for providing the data in Overill (2007).

References

- CMA (1990) *Computer Misuse Act 1990*, Available at: http://www.opsi.gov.uk/acts/acts1990/UKpga_19900018_en_1.htm, Accessed on 20 November 2008.
- CSMCFC (2008a) *Computer Forensics and Cybercrime Module Webpage*, Available at: <http://www.dcs.kcl.ac.uk/local/teaching/units/material/csmcfc/>, Accessed on 20 November 2008.

- CSMFC (2008b) *Computer Forensics and Cybercrime Module Syllabus*, Available at: <http://www.kcl.ac.uk/content/1/c4/92/11/CIMstructuremodules8.pdf>, Accessed on 20 November 2008.
- EnCase Forensic (2008) *Encase Product Information Webpage*, Available at: http://www.guidancesoftware.com/products/ef_index.aspx, Accessed on 20 November 2008.
- Gutmann, P. (1996) 'Secure deletion of data from magnetic and solid-state memory', *Proceedings of the Sixth USENIX Security Symposium*, San Jose, California, USA, pp.77–89.
- Locard, E. (1910) *Locard's Exchange Principle*, Available at: http://en.wikipedia.org/wiki/Locard's_exchange_principle, Accessed on 20 November 2008.
- Overill, R.E. (2007) 'Integrating cyberforensics into a forensic science masters programme', *Proceedings of the 1st International Conference on Cybercrime Forensics Education and Training (CFET 2007)*, Canterbury, UK, 6-7 September 2007, ISBN 1899253-041; Available at: http://www.dcs.kcl.ac.uk/staff/richard/CFET_2007.doc, Accessed on 20 November 2008.
- Overill, R.E. (2008) 'Development of a masters module in computer forensics and cybercrime', *Proceedings of the 2nd International Conference on Cybercrime Forensics Education and Training (CFET 2008)*, Canterbury, UK, 1–2 September 2008, ISBN 1899253-19x; Available at: http://www.dcs.kcl.ac.uk/staff/richard/CFET_2008.doc, Accessed on 20 November 2008.
- Overill, R.E. and Ferguson, R.I. (2007) 'Does computer forensics belong to computer science or forensic science?' Presented at the *3rd HEA ICS Workshop on Teaching Computer Forensics*, Northumbria, UK, 23–24 November 2007, Available at: http://www.dcs.kcl.ac.uk/staff/richard/HEA-ICS-TchCompFor_paper.pdf, Accessed on 20 November 2008.
- PJA (2006) Available at: http://www.opsi.gov.uk/Acts/acts2006/ukpga_20060048_en_1, Accessed on 20/11/2008.
- Stoll, C. (1988) 'Stalking the Wily Hacker', *Communications of the ACM*, Vol. 31, No. 5, pp.484–497.
- Stoll, C. (1990) *The Cuckoo's Egg*, Pocket Books, ISBN 0-7434-1146-3.