Cross-disciplinary Teaching of both Computer Forensics Students and Law Students Using Peer-Assessment in a Simulated Expert Witness Scenario

D. Chadwick, D. Gan, T. Vuong
Dept of Computing and Information Systems,
University of Greenwich,
London, UK
D.Gan@gre.ac.uk

E.Phillips
Dept of Law
University of Greenwich,
London, UK

***Abstract*—This paper describes a novel initiative of the Computing and Information Systems (CIS) Dept in conjunction with the Law Dept at the University of Greenwich. Postgraduate CIS computer forensics students, as part of their assessment, present their findings from a forensics investigation in front of a lecturer and up to five law students in a simulated expert witness testimony scenario. The law students are permitted to ask questions of the computer forensics students and eventually to give their assessment of the student's witness evidence and presentation. This approach was devised to encompass several pertinent pedagogic issues. Firstly, it is cross-disciplinary, combining as it does, input from two very different departments – an initiative that brings together not only students but also staff who would not otherwise meet. Secondly, it involves the use of practical social/professional skills for both sets of students, as the computer forensics students must present their findings with the skills required of an expert witness in a court setting while the law students must act as cross-examining counsel. Thirdly, this exercise involves the law students assessing the performance of the computer forensics students – an application of peer-assessment that heightens the involvement of both sets of students. Lastly, both sets of students are themselves graded, the computer students by their own forensics lecturer and the law students by their law lecturer, according to their performance in this exercise. The findings from questionnaires sent out to both computer and law students were extremely positive. Both sets felt that they had benefited from the experience and that it would aid their further studies and professional development in their respective areas.**

It is the opinion of the C-SAFE forensics-law collaborative team that this approach represents an educational innovation in its use of cross-disciplinary problem-solving and peer-assessment in a growing and increasingly significant domain worldwide (cyber forensics).

Keywords-component; Problem-based Learning; Cross-disciplinary collaboration; peer-assessment; Expert Witness evidence; Peer Assisted Learning; STEM teaching

I. INTRODUCTION

A. The Educational Rationale

'Traditional teaching, using formal instruction to fill supposedly empty vessels with knowledge organized by someone else, is often very ineffective. [Some] call it 'pour and snore'" [1]. Ever since the publication of the Cyber Security Strategy by the UK government [2], there has been an emphasis placed on new and improved training and education initiatives in the cyber security field [3]. As part of this initiative, the University of Greenwich has been teaching computer forensics to postgraduate students with a focus on the investigative process, rather than just on the forensic tools, using problem-based learning and practical exercises involving hands-on experience to ensure the students' understanding of the theory given in the lectures. A number of tools are used to show the students how to hide information, as well as how to find hidden information and files but tools alone do not make a forensics investigator [4]. An investigator must be able to defend their findings and methods of working under interrogation when acting as an expert witness in a court of law. Consequently, a new approach was considered. The team, relying on their previous educational research with computer forensics students such as in the use of Problem Based Learning [5], computing forensics assessments [4] and raising awareness with students new to forensics [6], decided on a cross-disciplinary collaboration with another department within the university, i.e. the Law Department. The concept was to involve students from both disciplines and get them working together in some way, especially if some element of peer-assessment could be introduced, in the area of expert witness testimony. Cross-disciplinary collaboration and peer-assessment are generally considered beneficial in higher education teaching. Exposing students to disciplines outside their main area of study broadens their outlook and extends their experience – it also brings them into contact with ideas, concepts and other students and staff they would not normally be exposed to; The same may be said for the lecturing staff themselves. Peer-assessment also gives students a glimpse into their own educational grading processes

and the common professional skill of establishing what others have achieved on a given task.

B Cross-disciplinary Approach

Research has demonstrated that student teams in cross-disciplinary teams have successfully been supported through concepts learnt in their respective disciplines and become more proficient in virtual communication (Brewer et. al., 2015 cited in Marshall Cavendish 2016) [7].

The computing forensics team had previously incorporated the use of legal case studies in their own presentation of technological issues but had not involved the Law Dept and its students more closely [8]. However, it was now recognized that there was a need for computer forensics students to gain experience of giving expert witness testimony and of being cross-examined by non-IT persons lacking familiarity with computing jargon. There was also possibly a need for Law students to appreciate the differences in perception of different witnesses and their professional need to develop listening, analysis and probing skills. So the exercise was constructed enabling computer forensics students to seek concealed evidence in a technologically demanding environment using all the forensic techniques taught to them, while the Law students would seek, through their questioning of the computer forensics students, to establish the strength of the evidence that they had found in establishing accountability. In addition, this exercise formed an integral part of their respective assessments for both sets of students.

C. Peer-assessment Approach

It is well-recognized that student learning is not only the province of tutors and PAL (Peer Assisted Learning) mechanisms are well known in the educational literature. It has been recognized, too, that students need to be motivated to support other students' learning – there is a need for structure through which they can work and it helps if the student mentors themselves receive some credit or recognition [9]. These factors were taken into account in the design of the exercise described herein. The exercise was to include elements of peer assessment, in that the Law students would interrogate the computer forensics student investigators to establish exactly what evidence had been found, how it had been found, and what significance was placed upon it as evidential artifacts. This required a feedback sheet (Appendix A) to be completed by the Law students as the interrogation proceeded; the comments and grading given by them on these sheets were used as input to the computer forensics students final grading for the exercise. In addition, the law students themselves were assessed according to their later write-up of the exercise and what they had learnt from it as part of their course Law of Evidence. It was considered that these tasks met some of the themes of good formative feedback as described by Irons [10]. It involved students in the feedback process, it was clear to students as to what the feedback was trying to achieve and how it contributed to their learning.

D The Stages of the Exercise

Based upon the team's previous experience in planning forensics projects [11] and working with adult learners [3] an exercise using a case study scenario was constructed along with a cross-disciplinary collaborative approach using peer-assessment was designed. The entire exercise was designed in three stages as shown in Table I.

TABLE I. STAGES OF THE EXERCISE

Stages of the Exercise		
Stage	***Student Cohort***	***Task***
1.Case study forensic investigation	Computer forensics students working individually	Work on practical case study using suspect's hard drive copy. Variety of forensic tools used uncovering hidden/obscured artifacts of evidence and information on possible suspects
2.Peer assessment - expert witness simulation	Computer forensics students and Law students together (peer-assessment)	Expert witness testimony simulation involving interrogation of computer forensics students by law students on their forensic findings and their opinions on possible suspects. Law students to provide feedback on computer forensics students' performance (Appendix A).
3. Student feedback on the exercise	Computer forensics students and Law students Individually	Questionnaire (Appendix B) to computer forensics students.

II. STAGE 1 : CASE STUDY FORENSICS INVESTIGATION

The case study is designed to test the computer forensics students' ability to apply the theory they have learned throughout the course. It is based around a simulated crime. This year the case was terrorism and the plot revolved around a well-known eco-terrorist who planned to poison world leaders at the 2017 G20 conference in Hamburg to raise awareness of animal cruelty that takes place in lab experiments around the world. There were other sub-plots around blackmail to gain recruits for the cause and drug dealing to fund their activities. The case includes travel documents and hotel bookings in Hamburg, along with hidden plans of the ventilation systems in the rooms. A few students used an Internet search to identify that the G20 meeting was going to take place in this hotel and then linked all the plans up to identify that the suspects were planning to poison the air-conditioning units to kill the world leaders at the event.

To make the experience as realistic as possible the students receive information (bios) on the criminals involved (names, addresses, etc.), how and when they were apprehended and how the evidence was collected. The forensic evidence given can be in the form of a USB stick, an ISO image or as a forensic image (.E01) format which can be loaded directly into forensic tools such as EnCase or FTK (Forensics Tool Kit).

The evidence is structured so as to have a number of easy artifacts, some slightly harder and then some very challenging ones to stretch the more able students. The easy artifacts can be found either through observation or by using methods and/or tools that the students have practiced in the labs e.g. a document with white text on a white background; a picture covering text; a password observed in a picture; a password being the protected file's actual name. Medium artifacts are characterized as requiring additional skills. In this case, examples are files with

passwords which the student has to crack, but the password is taken from a word in the bio, such as the criminal's surname or address; the use of hashing, binary or ASCII codes instead of plain text passwords. This also requires the use of additional tools. The hard evidence requires the students to go beyond the labs that they have been practicing with and apply concepts which will require research or innovation. Examples here are the use of hidden files, steganography to hide important documents or emails in images and video files and the use of passwords which require a password cracking tool to reveal them.

The marks given for the evidence found however did not depend on the students finding all the evidence, but more on how effective they were at recognizing the significance of the information and how it was communicated to the "court" i.e. the Law students.

III. STAGE 2: PEER ASSESSMENT – EXPERT WITNESS SIMULATION

Appendix A contains the feedback sheet filled in by the Law students as they interrogated the computer forensics students' Expert Witness evidence. As the Law students have no prior knowledge of forensics "jargon", the "Expert Witness" must explain the evidence that they have found without using any technical terms. If they do mention something that the Law students do not understand then they are stopped and asked to explain the term used. This often causes them some difficulty. The highest scoring students tend not to use any jargon and explain the evidence they found in plain English.

The computer forensics students were briefed on how to present evidence as an expert witness during the lectures. They must look smart and be confident in their findings. They must also be able to explain any technical points they raise in a non-technical way.

The Law students are briefed to give marks for categories such as:- smart and professional appearance; confidence in presenting; not using jargon or technical terms; did they find enough information to convince the markers that this person was guilty of the crime.

IV. STAGE 3: STUDENT FEEDBACK ON EXERCISE

Both the Computer forensics and the Law students were given questionnaires to elicit feedback on what they thought of the exercise. The questionnaires were worded differently for each and statistics compiled on how successful and useful the exercise had been.

A. Questionnaire Findings: Computer Forensics Students

The questionnaire distributed to the Computer forensics students and detailing their responses to this exercise is to be found in Appendix B. It consists of seven questions to which the student was asked to respond on a Likert scale from 1 (I do not agree) to 5 (I fully agree). The questions were devised into those referring to skills and learning outcomes useful - in the students' possible future professional environment and those having usefulness in the current academic environment. In total there were three questions relating only to the future professional environment (P), two questions only to the current academic environment (A) and two questions encompassing both environments (PA).

TABLE II. RESULTS OF THE QUESTIONNAIRE

		LIKERT SCALE				
Questions	***Prof'l or Academic***	***1***	***2***	***3***	***4***	***5***
It gave me a useful insight into being an expert witness.	P			3	6	8
It gave me experience of being able to express myself clearly to a listening audience.	P			1	11	5
It helped me to learn that I have to really know my stuff before being questioned.	P and A			1	2	14
The law students made me realise different listeners form different impressions of what I say.	P and A		3	2	9	3
It gave me useful experience on answering pertinent questions on the spur of the moment	P			2	10	5
I believe this will help with my computer forensics studies.	A		1		8	8
I enjoyed the whole session and suggest it should be repeated with next year's students.	A				6	11
Total Replies		**0**	**4**	**9**	**52**	**54**

The overall results of the questionnaire from the 17 respondents are shown below in Table II.

Overall the results show a strong bias at the 'I fully agree' end of the Likert scale (5) which indicates strong positive outcomes for the exercise, as seen in Fig. 1. No replies were obtained in category 1 'I do not agree' and few (only 4) in category 2. Overall, the most positive categories (4 and 5) had a total of 106 out of 119 responses, which is 89% satisfaction. Question 7 certainly had the most positive and was a strong indication to staff that they had created a most useful exercise with the students. Questions 2, 3 and 5 had 16 replies at 4/5 category suggesting that the students had understood the wiser implications of the distinct learning outcomes that could be of use in later professional life.

B. Questionnaire Findings: Law Students

A similar questionnaire was distributed to the Law students asking for their responses to this whole exercise. The replies have not been presented in this paper as this paper is primarily concerning computing science education – although results for these students will be presented in a Law oriented conference at a later date.

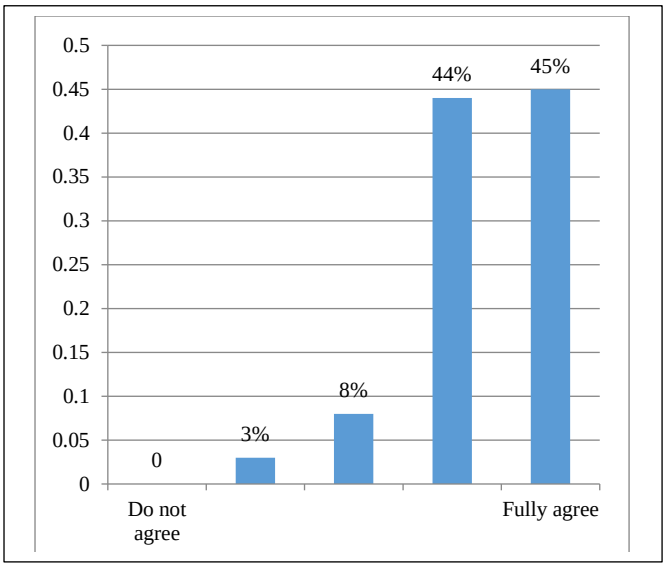

Figure 1. Analysis of replies of Computing Students Questionnaire

V. CONCLUSION

Overall, this collaborative and assessment approach has identified synergies created across disciplines as a result of working together on scenario design and implementation. It has addressed the tensions generated between the pedagogical requirements of different sets of lecturers and the design objectives of creating an interesting scenario to capture the interest and involvement of different sets of students [12].

Peer learning is an important concept for students [13] as the benefits of students learning from each other should not be underestimated, particularly when the students are from two entirely different disciplines, as in this case. It should be pointed out that the law students were exposed to concepts that they had never encountered regarding digital forensics. Alternatively, the computer forensics students had never discussed their findings anyone except their own peer group, so this was quite a revelation for them.

Peer assessment is the process of learning by giving others feedback on their work. This is a concept which we use in this exercise which is particularly beneficial in IT based courseworks as identified in [14]. Rietsche et el. (2017) empirical assessed the effect on the ability of IT students to give feedback and to receive peer assessment from their fellow students on the overall learning process and demonstrated that the students had substantially benefitted from this process [14].

The questionnaire results were very positive for both Computing and Law students. The fact that both sets of students benefitted was a significant finding.

A. Computing Forenisc Students

In particular, the results for the computer forensics student questionnaire (Appendix B) far exceeded the expectations of the computing staff. The results show a positive result that is statistically significant at the 95% level. However, prior to the exercise it had been thought that students would resist such a personally demanding scenario putting them on display, so to speak, in front of several others and forcing them to not only know the full detail of their own work but to be able to defend it in a non-technical way. It was encouraging to find that they appreciated the more real-world approach of this exercise. It should also be mentioned that anecdotal feedback from these students attending interviews indicates that employers highly value the simulated realism of this whole exercise.

B. Law Students

The Law students, too, had a highly positive reaction to this collaborative scenario. Opinions collected anecdotally at the time showed that they enjoyed the experience of practical witness interrogation where the ‘witness’ was a complete stranger and not a fellow Law student. They also made it clear that they appreciated the opportunity to learn computing jargon and forensics procedures that they were almost certainly to meet in reality sometime in their future careers.

C. The Staff

An important element of this entire exercise, and one which was almost overlooked,was the responses of the staff. Although not specifically surveyed it was clear that all staff gained from meeting lecturers from another discipline, from giving their own students a wider and novel experience, and from seeing their own subject areas in a wider context. Future work on this exercise will include formal questionnaires to staff involved in the exercise and to other non-involved staff to elicit their opinions.

D. The Future

For the immediate future, this exercise will be repeated with other cohorts of computer forensics and law students. It would be interesting to see if the findings herein would be replicated with other students and how the exercise might further be developed.

For the cross-disciplinary element, now that relationships between staff in the Law and Computing departments have been established, there is the possibility of closer liaisons and collaboration in other areas and other cohorts of students. It is clear to the collaborating team that both sets of students and staff have much to gain by working together. For the peer-assessment element, there is every likelihood that the techniques will be explored, extended and refined over time.

For the far future, there is also the possibility of the building of a generic model of cooperation; such a model may form the basis of a defensible pedagogic model which may prove useful beyond the Law-Computing collaboration to one useful for STEM (Science, Technology, Engineering, Mathematics) teaching generally.

Overall, the collaborative team believe that their approach using cross-disciplinary peer-assessment is an innovative educational experience for all involved students and for staff.

REFERENCES

[1] Perry N., Sherlock D. 2008; Quality Improvement in Adult Vocational Education and Training: Transforming Skills for a Global Economy; Kogan Page ISBN 978-0-7494-5103-5

[2] Clemente D., (2011); The UK Government Today Released It's 2011Cyber Security Strategy. International Security Programme, Chatham House, UK, 25 Nov 2011: http://www.bbc.co.uk/news/technology-1589377

[3] Gan D., Chadwick D., Frangiskatos D, Loukas G (2012); Short Course Teaching of Cyber Security To Mid-Career Physical Security Professionals With Limited Academic Background; 6th International Conference on Cybercrime Forensics Education & Training, Canterbury Christchurch University, Sept 2012

[4] Gan D., Chadwick D., Frangiskatos D. (2010); Development of Challenging Assessments for Computer Forensics Students;8th Annual Teaching Computer Forensics Workshop(HEA-ICS), Programme Chair: Alastair Irons; Nov, Sunderland University,UK

[5] Chadwick D. & Gan D. (2011a); An Educational Paradigm (PBL) for Teaching Computer Forensics; HEA-ICS Conference, University of Derby, February 2011

[6] Chadwick D., Gan D., Frangiskatos D. (2016); 'Awareness Raising' of CyberSecurity in HE Taster Sessions; National Conference on Learning and Teaching in CyberSecurity, 15June2016 Maple House, Birmingham,UK

[7] Marshall Cavendish Education 2016; How Effective is a Cross-disciplinary Approach to Teaching Science?; Marshall Cavendish website article posted 6th September 2016, https://spark.mceducation.com/201609/06/how-effective-is-a-cross-disciplinary-approach-to-teaching-science/, accessed 2ndMay2017

[8] Chadwick D., Gan D., Frangiskatos D. (2015); Teaching Forensics Principles through Legal Case Studies; 11th Annual Teaching Computer Forensics Workshop; 19th November 2015,Sunderland University, UK

[9] Fry H., Ketteridge S., Marshall S. 2009; A Handbook for Teaching and Learning in Higher Education : Enhancing Academic Practice 3rd Edition; Routledge ISBN 978-0-415-43464-5

[10] Irons A (2007); Enhancing Learning Through Formative Assessment and Feedback (Key Guides for Effective Teaching in Higher Education); Routledge ISBN10 0-415-39781-2

[11] Chadwick D. & Gan D. (2011b); What Next For Computer Forensics Projects? 9th Annual Teaching Computer Forensics Workshop (HEA-ICS): Programme Chair Alastair Irons; Nov2011, Sunderland University, UK

[12] Rooney P., O'Rourke K.C., Burke G., Mac Namee B., Igbrude C., (2008); Cross-disciplinary approaches for developing serious games in Higher Education Frameworks for Food Safety and Environmental Health Education ; Dublin Institute of Technology Dublin, Ireland

[13] Boud, D., Cohen, R. and Sampson, J. eds., 2014. Peer learning in higher education: Learning from and with each other. Routledge.

[14] Rietsche, Roman; Lehmann, Katja; Haas, Philipp & Söllner, Matthias (2017) The Twofold Value of IT-Based Peer Assessment in Management Information Systems Education. In: 13th International Conference on Wirtschaftsinformatik (WI), 12-15.02.2017, St. Gallen, Switzerland

Appendix A: Peer-assessment feedback sheet completed by Law students

Jury Member Evaluation
Mock Trial

Student Name ……..

Student Number ……

Presenting Evidence
Did the Expert witness convince you with the evidence that was presented? YES / NO

Please grade by circling

	I do not agree ←				→ I fully agree
Confident	1	2	3	4	5
Knowledgeable	1	2	3	4	5
Convincing	1	2	3	4	5
Sufficient evidence found	1	2	3	4	5
Can present the evidence	1	2	3	4	5
Explained the evidence when challenged	1	2	3	4	5
Smart and professional	1	2	3	4	5

APPENDIX B: Questionnaire given to computer forensics students

Dear Computer Crime & Forensics Student,

Recently you participated in a simulated courtroom session as part of your COMP1541 Computer Crime & Forensics coursework. You answered some questions from a lecturer and possibly some Law students. We were hoping you would care to comment on this experience for our future course development and as part of our educational research programme here in C-SAFE.

1. It gave me a useful insight into being an expert witness.

Please circle figure from 1 to 5 to rate your agreement:

I do not agree				I fully agree
1	2	3	4	5

2. It gave me experience of being able to express myself clearly to a listening audience.

Please circle figure from 1 to 5 to rate your agreement:

I do not agree				I fully agree
1	2	3	4	5

3. It helped me to learn that I have to really know my stuff before being questioned.

Please circle figure from 1 to 5 to rate your agreement:

I do not agree				I fully agree
1	2	3	4	5

4. The law students made me realise that different listeners form different impressions of what I say.

Please circle figure from 1 to 5 to rate your agreement:

I do not agree				I fully agree
1	2	3	4	5

5. It gave me useful experience on answering pertinent questions on the spur of the moment.

Please circle figure from 1 to 5 to rate your agreement:

I do not agree				I fully agree
1	2	3	4	5

6. I believe this will help with my computer forensics studies.

Please circle figure from 1 to 5 to rate your agreement:

I do not agree				I fully agree
1	2	3	4	5

7. I enjoyed the whole session and suggest it should be repeated with next year's students.

Please circle figure from 1 to 5 to rate your agreement:

I do not agree				I fully agree
1	2	3	4	5

Thank you very much. Please hand your completed form (but do not give your name) to any member of the C-SAFE team as shown below. And many thanks for your help in this matter.

David Chadwick, Diane Gan, Tuan Vuong, Edward Phillips
Cyber-**S**ecurity, **A**udit, **F**orensics **E**ducation Centre