An Educational Paradigm for Teaching Computer Forensics

David Chadwick, Diane Gan, Dimitris Frangiskatos

C-SAFE (Computer Security Audit Forensics Education) Centre

School of Computing & Mathematical Sciences, University of Greenwich, London, England, SE10 9LS

***Abstract* — Teaching Computer Forensics to students at postgraduate and undergraduate levels is a challenge. Creating an assignment that is both realistic and also helpful to students when pursuing careers in this competitive area is also a demanding task for the lecturer. A problem-based learning (PBL) strategy has been used to increase the employability of the students, by designing a real-world problem for the students to solve. It can be shown that this enhances the employability skills of the students when it comes to finding jobs. The coursework is based around a case study. To add an extra dimension to the assessment we involved final year Law students from the School of Humanities, Law Department, to act as jury members and also to help to cross-examine the postgraduate students while they presented their findings in the role of an Expert Witness. This created at the same time a valuable exercise for the legal students in the context that evidence presented in courts is increasingly computer-based evidence. This paper discusses the preparation of the evidence files, how employability is enhanced by the use of a PBL approach to teaching, the process of evaluating the results of the students work and concludes with an overview of the student experience for all students involved.**

1. Introduction

At the University of Greenwich we have been teaching computer forensics at Masters level for three years. Teaching computer forensics to postgraduate students is a challenging topic. The core course is called Computer Crime and Forensics. This is taught using a two hour lecture and a two hour lab. Our approach to teaching this subject has always been to focus on the investigative process, rather than just on the forensic tools, using problem- based learning (PBL). Practical exercises involving hands on experience are key to ensure the students' understanding of the theory given in the lectures. We do use a number of tools to show the students how to hide information, as well as how to find hidden information and files. It is also important that students understand the capabilities and limitations of these tools. But tools alone do not make a forensics investigator.

An example of PBL is the assessment that we set for the students studying Computer Crime and Forensics. We have taught the students basic skills but they then have to take this a step further and think for themselves in order to solve the "case".

The assessment for this course was built around an imaginary case study, designed to give a feel for a real-life forensic assignment, as well as testing students' skills in all aspects of a forensics investigation. The setup was that a member of the research and development (R&D) team working for Mitsubishi Motors' was suspected of selling industrial secrets to a rival company regarding a new prototype that was under development. The suspect's USB stick had been removed from his computer while he was at lunch. A forensic read- only copy of the USB stick had been made and verified, and the USB stick had been returned to the "suspect's" computer so as not to arouse his suspicions, as it was suspected that there were other staff members also involved. The read- only copy of the USB stick was then made available to all students as an ISO image for them to download. The students were instructed to search for "evidence" to prove that the "suspect" was in fact stealing company secrets. A number of pieces of evidence had been concealed in a variety of different ways, some easy to identify and others much harder to identify. They were permitted to use any tools they thought appropriate to evaluate the files, but the Chain of Custody was to be maintained at all times. The students were then required to write a report on their findings. The report was structured around a generic template that we supplied and which they were required to modify slightly to suit the case in hand.

The final part of the assessment for each student, was to present their findings in a "court room" situation, as an Expert Witness. This is an important aspect of being a computer forensic investigator. It also emphasised the additional skill requirements of being able to present forensic evidence under cross-examination in a court environment, as well as giving practical focus to the way in which the evidence was gathered. The students were instructed not to use any jargon, as Judge Judy would not understand "techno-speak". To add realism to this we contacted the Law Department and requested the help of a number of final year Law students to act as jury members and to also help with the cross-examining of the postgraduate students regarding their testimony. By including the Law students, we hoped to simulate a slightly more realistic experience, comparable with what would be found when presenting in front of a judge and jury in a real court case. We also hoped that this would also be a valuable exercise for the Law students as well, as it exposed them to a completely new area that they had never encountered before. In this day and age the evidence presented in courts is becoming increasingly computer-based, and they found this a fascinating exercise. For the undergraduate students we felt that they should also present their findings but this was done in front of the lecturers, with no additional people present.

This paper discusses the employability-enhanced PBL approach to teaching, the preparation of the evidence files, how the students' work was evaluated and concludes with an overview of the student experience for all the students.

The rest of this paper is laid out as follows. Section 2 describes the creation of the evidence files. Section 3 explains our Employability-Enhanced PBL approach to the teaching of computer forensics at the University of Greenwich. The students' results are discussed in section 4 and section 5 describes the student experience. Section 6 is the conclusion.

2. Employability-Enhanced PBL Approach To Teaching

The Confederation of British Industry said it would be "broadly in favour of universities including more workplace and employability skills in undergraduate courses" (Guardian, 2011)

The forensic team at Greenwich, who are all members of the C-SAFE team deliberately set out to create a course that reflected the real world and helped the students to learn workplace and employability skills that would aid them at job interviews. There are two ways in which the Greenwich C-SAFE team designed workplace and employability skills into their digital forensics taught courses – see fig 1.

Firstly, the course was designed to enable students to gain up to two employment enhancing artefacts which could be mentioned in the student's CV and/or presented at job interviews.

Secondly, the coursework case study problem was closely based upon real-world forensic investigations and was deliberately designed to address issues of data-insufficiency and data-irrelevancy which characterise real digital forensics investigations. Such exposure enhances workplace and employability skills.

2.1 Employment Enhancing Artifacts

Pre-Case Study

The entire teaching was based around the case study problem presented for the coursework assessment. The Greenwich C-SAFE team have established contacts with Guidance Software, who produce the EnCase industry-standard Forensic tool, and, also, with a forensic practitioner with experience in industry. These represent the real-world inputs into the teaching and the coursework problem. The tutorials given to students gave extensive use in Encase to enable proficiency in use of the tool in preparation for when the case study problem. Similarly, the industry practitioner was invited along to give a guest lecture to students on the role of the forensics investigator and especially as expert witness giving evidence in a court of law.

Case Study

The case-study problem, itself , had three stages:

Stage 1: Forensic Analysis Using EnCase

The students were presented with a written explanation of the case study in which the alleged suspect was an employee of a motor manufacturer and was suspected of being a participant in an industrial espionage event whereby copies of confidential plans of a new vehicle were being taken and supposedly passed to a competitor. The students were given an ISO image of the alleged suspect's hard drive and were asked to analyse the data in the image and to identify relevant or potentially relevant artefacts concerning the suspect's involvement or otherwise. Students were required to document their forensic strategy and their findings using the EnCase tool for which they were adequately prepared with basic skills in the preceding tutorial sessions (Fig 1).

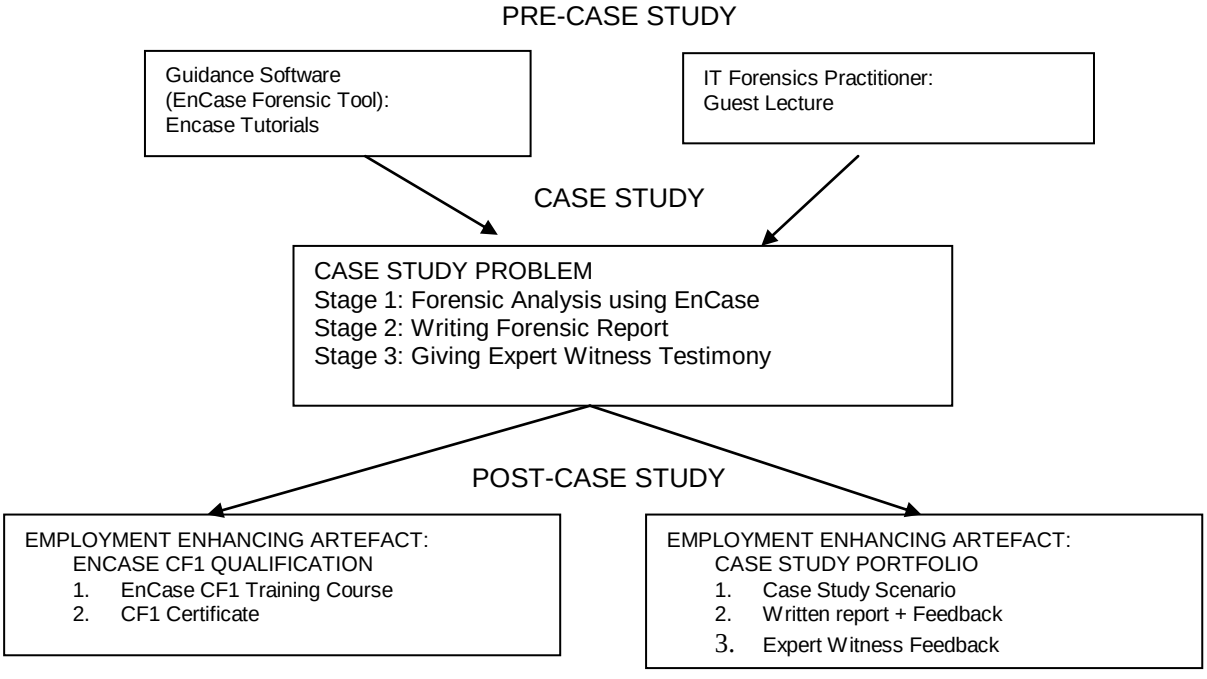

Fig 1 : Model of C-SAFE Industry-Based PBL Approach

Stage 2: Writing the Forensic Report

Students were required to write a concise but complete report detailing the evidence they had uncovered, if any, and a statement of whether they consider the suspect was involved in the alleged espionage event or not. The format and content of the report was based upon guidance given by the guest speaker.

Stage 3: Giving Expert Witness Testimony

Students were individually required to give expert witness evidence in a simulated courtroom session in which they were cross-examined by a tutor posing as legal counsel and also by students from the University of Greenwich law department. The students were guided in their witness approach by hints given in the guest speaker's lecture.

Post Case Study

There were two employment enhancing artefacts from this case study.

Firstly, students, having completed a set of EnCase tutorials and gained experience in its use through a number of real-world problem simulations, are able, if they wish, to take the EnCase CF1 (Computer Forensics 1) course approved by Guidance Software, which is delivered by the C-SAFE team. Successful students are given a certificate underwritten by Guidance Software as an artefact which they can mention in their CV and discuss at job interviews.

Secondly, students were encouraged to put together an employment portfolio containing the original case study scenario description, their own report, and tutor feedback on their report and expert witness session. Students were therefore equipped with an artefact that they may present at job interviews to show their personal proficiency in tackling a real forensic case.

2.2 Enhancing Workplace and Employability Skills

It was decided by the tutor team that the approach to learning and assessment would be based on the widely-recognised PBL (Problem-Based Learning). PBL is considered to have positive effects on student learning. First, it is contextually valid as problems are taken from professional or academic practice and students acquire knowledge around these problems. There are indications that students really do learn to solve problems in a better way as it has a strong motivating effect with little emphasis on perceived 'dry' theory and more emphasis on exciting practitioner elements (VanBerkel H. J. M, Schmidt H.G, 2000). In addition, it is a teaching system designed to emulate professional practice in a way that assessment is performance-based, holistic, and permitting students to input their own thoughts and decisions (Biggs, 1999 cited in LTSN Assessment series 13, 2010; p7).

In PBL the focus is on :

1. Organising the curricular content around problem scenarios rather than subjects/disciplines.
2. Having problem scenarios that reflect real world situations.
3. Encouraging students to learn by themselves as they seek further knowledge.
4. Having staff engaged as 'learning facilitators' rather than 'front of the class' pedagogists.
5. Encouraging students to learn together and share the further knowledge research process.

The emphasis in this paper is on the first two factors concerning the use of problem scenarios that reflect real world situations.

2.3 Designing A Problem Scenario That Reflects Real World Situations

In terms of constructing problems for student learning, tutors have combinations of data-irrelevancy/data-insufficiency available to them – see Table 1. However, real world digital forensic investigations are characterised by two properties which are, for convenience, called Data-Completeness and Data Irrelevancy. Table 1 shows combinations of these two qualities that can arise and a quick examination shows that most academic classroom type questions are of the RC or RI type whereas most real-world problems are of the II type.

Data-irrelevancy?	***Data-Completeness?***	
All data relevant	*Complete – all relevant data for solving problem*	*RC*
All data relevant	*Incomplete – not all relevant data is given*	*RI*
Irrelevant data	*Complete – all relevant data for solving problem*	*IC*
Irrelevant data	*Incomplete – not all relevant data is given*	*II*

Table 1: Problem Characteristics

Data-Completeness is the property of a problem whereby all the data/information to solve the problem is available to the student within the initial problem scenario. This is the normal classroom academic problem in that most questions for students contain all the data the student needs. However, data-incompleteness is an issue for the student in that, firstly, they must be able to exhibit awareness as to whether the necessary data to form a conclusion is available or missing. If the student is aware that data is missing, then secondly, they must choose how to deal with the situation. Typically, this reduces to one of three courses of action: to seek the actual missing data by further research, to deduce the missing data using some kind of logical deduction process or to make a qualitative assumption about what the missing data might be. In all cases the student must be able to describe and justify their modus operandi if called upon.

Data-irrelevancy is the property of a problem whereby extraneous data, that plays no part in the problem solution, is presented within the problem scenario. For the student,

this is an issue in that they must be able to exhibit discernment in terms of what is relevant and what is not or basically just 'noise'.

The problem designed for students by the C-SAFE forensics team was of the II type, i.e. it contained some of the data the students needed (but not all so they had to go looking for further data) and contained irrelevant or extraneous data (so they had to wade through material that did not apply).

3. Evidence Creation

The evidence was based on an imaginary industrial espionage scenario for a known automotive company. The students were handed an ISO image of the original evidence files. This was selected due to its portability. The students were told that the person dealing with the investigation internally, a security manager, had produced the image from the original media. To be noted here was that part of the exercise was to demonstrate that often direct access to the evidence might not be possible before a case is built. Assumptions have to be made and working with evidence which has not been collected with well- known forensic software tools by people without a computer forensics background is possible.

The students had been practicing all term on how to hide and recover files and information. They had also had experience of using a number of tools, both commercial and open source. These include EnCase (Guidance Software), FTK (Access Data), hex editors, hash generators and a number of other open source tools, such as steganography tools and the MasterKey forensic tool.

However the rationale behind this case was that the student should be able to work on the evidence using commonly available basic Open Source tools such as a hex editor with memory and disk- viewing capabilities. It is our belief that having graduates who simply know how to use complex tools such as EnCase and FTK is not enough to produce competent computer forensic scientists.

The creation of the evidence files was key to this assessment. The evidence was divided into three categories, with some evidence being very easy to find and all students should have found these files, some that was slightly more challenging and some that was very challenging. We did not expect many students to find all the evidence. We also wanted this investigation to be an enjoyable activity. When building the evidence we tried to think as our imaginary industrial espionage culprit. The profile of this individual is was someone who worked at the research department of a well- known and highly competitive automotive company and tried to sell blueprints of a rally car gearbox to a well-known rival company. We assumed that the perpetrator moved data in and out of the company on his company-provided USB stick which is scanned day by day by the in-house anti-everything security tools.

The suspect's files included a number of personal documents, photos, some video footage, software applications, copyrighted material, email communication and archived files. A number of "hints" were planted that students could use to help them progress their investigation. These were supposed to be the perpetrator's comments or "post-it notes" that were to be used by the rival company to extract the stolen information hidden in the files of the USB stick.

Some "hints" were quite simple to identify and included changed file extensions (mangled files), text having the same colour as the background, phrases in different languages and encoded data which even a trainee would be able to pick up. An example here is that in one of the compressed archives which contained a number of incriminating encrypted data the following comment aGlkZGVuIGZpbGVzIGluc2lkZQ== was included. This is base64 for "hidden files inside". In some cases messages were hidden at "the end of the road" so that the students could experience what a real investigators experiences with evidence that appears relevant only to discover that they are of no importance. An example of this was that inside a doubly- compressed archive with basic password protection - which was the name of the file - there was a word document which appeared empty but on its footer contained an encoded message. This read d2hhdCB5b3Ugc2VlIGhlcmUgaXMgbm90IGltcG9ydGFudCBzbyBsb29rIGVsc2V3aGVyZQ==. This is base64 encoding for "what you see here is not important so look elsewhere".

It is quite important to point out that the use of automated computer forensic tools made a number of students overlook basic clues which one would expect that to have been picked up quite early.

There were also some "circumstantial evidence" files included in the image. These included the presence of some e-books and password cracking, hacking and anti-forensics techniques. There were also some of the tools that had been used to hide the evidence such as Steg-hide, Glue, Truecrypt. These were intended as a "hint", but many students did not pick up on this or mention it in their report. A few spoke about this in their presentation, but concluded that this proved the person's guilt, for which they were duly "shot down".

Unfortunately for some, the tools became more important than the investigation. So much so, that certain evidence files were missed completely by some students because in order to identify the evidence a little bit of observation was all that was required, along with basic software tools such as MS Paint and MS Notepad

4. Results

The students submitted a written report of their findings, using a given template. Some found using the template quite challenging. Not all the headings were relevant to this case and some students deleted sections, which lost them some marks. The top students did keep to the standard structure.

The majority of the students chose to use FTK for their investigation, even though they had access to EnCase in the university labs. When asked about this, their reasoning was twofold. They found FTK easier to use than EnCase. Also they could download a free version of FTK that meant that they could work on the coursework at home, as EnCase was only available in the university labs.

Virtually all the students found the "easy" evidence, with the best students finding nearly all the evidence, even the most challenging, such as the encrypted and password protected files.

The second part of the coursework was the Expert Witness testimony. Many of the students found this very challenging. The addition of the Law students gave the exercise an extra dimension. They were not "techie" students, so when any of the forensics students began to talk in a technical way, they were stopped immediately and asked to explain what they meant by a term or a phrase that they had used. This did throw some of them, as they were using terms that they could not adequately explain, in an attempt to impress the "jury".

The students were assessed on things such as their appearance – did they look smart and project a professional demeanour. Were they able to answer questions confidently and competently and of course, the content of their evidence. They lost some marks for being too "techie" and not explaining anything they were discussing at the right level so that the Law students could understand. The marks given for each presentation were a combination of the lecturer's mark and the "jury's" marks. The Law students also wrote comments regarding each student's performance and were asked to indicate if they thought that this "expert witness" did convince them that the defendant was guilty.

When this course ran for the first time, there was some anxiety amongst the team about how the students would perform. The average coursework mark for the class was 55.133%. The top student got 97% for the coursework. A total of 44 students passed out of the 50 who were registered for the course. Four students failed either because they did not hand in any coursework or because they failed to attend the exam.

Overall the teaching team were very pleased with the way the students tackled the coursework. It was quite challenging and completely different from anything the students had previously done.

5. The Student Experience

There were two sets of students to consider here. The first set was the Masters students from the School of Computing and Mathematical Sciences (CMS) who were being assessed and for whom the assignment was worth 50% of their course grade. The second set was the Law students who were helping with the evaluation of the expert witness testimony. We will discuss each set separately.

The CMS Students (the Expert Witnesses) were formally questioned on their impressions of the experience. Of the original 50 students in this cohort, 36 took part in this survey. They were asked three questions and replies were obtained as follows (see Table 2).

Questions	Responses
1. Did you enjoy the experience – Yes/No?	67% (24 of the 36) said Yes
2. Did you learn from the experience – Yes/No?	100% (36 of the 36) said Yes
3. Do you have any suggestions on how it might be improved?	Several suggestions were made including: More preparation time to be given

Table 2: Questionnaire Results

However, the most surprising findings were those from the Law students. No formal survey was given to the Law students – our main focus was the CMS students. However, to the surprise of the team, the Law students themselves voluntarily offered feedback on how much they had enjoyed the experience. They were questioned informally and of the nine students involved, all of them reported verbally that they had enjoyed the experience and had learned something. The main learning outcomes were reported as:-

1. They had found it a useful experience to actively cross-examine an expert witness

2. They had learned some useful computer jargon hitherto not part of their Law studies,

3. They had learned that computer-based crimes could be difficult and complex to understand

So, it may be possible that the Law students, who were not the main recipients of the PBL approach, developed some employability and workplace skills for themselves. Further research needs to be done in this respect.

6. Conclusion

This paper has presented an overview of the philosophy behind the development of the undergraduate and post graduate programmes in computer forensics at the

University of Greenwich. We have discussed the development of the course work for the core course Computer Crime and Forensics using the PBL paradigm and the innovative way that we assessed that coursework. An overview of the development of the case study for the coursework and the process of assessing the students has been presented. The three parts of the coursework, which were the analysis of the evidence, the report writing and the presentation as an expert witness have been discussed. The student experience has been reported, which was very positive. In the Annual Student Survey, 86% of the students said that they would recommend this course to a friend.

Our PBL approach has proved to be a success in the teaching of computer forensics. Our three tutor approach to the teaching has also contributed to making this new discipline a success. We intend to continue with this paradigm and, build upon it with more 'facilitation' sessions and more in-depth follow up questions. We also intend to strengthen our links with the Law Department in order to enhance the contribution of the Law students.

The PBL approach adopted by the C-SAFE team has placed emphasis on the design of the 'problem' itself which has succeeded in being soundly academically based in taught materials, constructed around a real-world scenario, and challenging for the students in its intricacy and detail. The 'problem' was well drawn out, extending from the collection of original data, to its analysis, reporting upon and then presentation in a courtroom setting. In so doing many skills, academic, practical, personal, and professional have been addressed. The student experience has been enhanced and their employment prospects have been improved.

REFERENCES

Barrows H (1985); How To Design A problem-Based Learning Curriculum For The Pretechnical Years, New York NY, Springer

Eraul M (1990); Identifying the Knowledge That underpins Performance. In Black H(editor) Knowledge and Competencies: Current issues in training and education, London. Scottish Council for Research in Education in association with the University of London.

Goleman D (1996); Emotional Intelligence – Why It can Matter More Than IQ; Bloomsbury Publishing, London 1996

LTSN Assessment Series 13, 2010; A briefing On Assessment in Problem-Based Learning; MacDonald R, Savin-Baden M; http://www.bioscience.heacademy.ac.uk/; 9th Nov 2010

LTSN (2010); A briefing On Assessment in Problem-Based Learning; MacDonald R, Savin-Baden M; LTSN Assessment Series 13 on www.bioscience.heacademy.ac.uk/; 9th Nov 2010

Price B (1999); An Introduction To Problem-Based learning; Nursing Standard vol.13 June 1999

VanBerkel H. J. M, Schmidt H.G, 2000; Motivation to commit oneself as a determinant of Achievement in PBL, Higher education 40:231-242, 2000; Kluwer Academic Publishers, Netherlands]