Higher Education Pedagogies

ISSN: (Print) 2375-2696 (Online) Journal homepage: http://tandfonline.com/loi/rhep20

Problem based learning in digital forensics

Alastair Irons & Paula Thomas

To cite this article: Alastair Irons & Paula Thomas (2016) Problem based learning in digital forensics, Higher Education Pedagogies, 1:1, 95-105, DOI: 10.1080/23752696.2015.1134200

To link to this article: http://dx.doi.org/10.1080/23752696.2015.1134200

HIGHER EDUCATION PEDAGOGIES, 2016
Vol. 1, No. 1, 95–105
http://dx.doi.org/10.1080/23752696.2015.1134200

Problem based learning in digital forensics

Alastair Irons[a] and Paula Thomas[b]

[a]Computing, Engineering and Technology, University of Sunderland, Sunderland, UK; [b]Computing & Mathematical Sciences, University of South Wales (Glamorgan), Glamorgan, UK

ABSTRACT

The purpose of this paper is to compare and contrast the efforts of two universities to address the issue of providing computer forensics students with the opportunity to get involved in the practical aspects of forensic search and seizure procedures. The paper discusses the approaches undertaken by the University of Sunderland and the University of South Wales (Glamorgan) to give the students the opportunity to process a case from the crime scene through to the court room. In order to do this both institutions adopted a problem-based learning (PBL) approach – to reflect real-world solutions and encourage students to work in groups to seek further knowledge and understanding of the various processes and procedures – in particular the steps around search and seizure of digital evidence from a crime scene. The PBL activities at Sunderland and Glamorgan were designed in order to help the students understand the processes of digital crime scene analysis and search and seizure procedures and to give them the opportunity to put into practice their digital forensics techniques. Both exercises were designed to give the opportunity to solve realistic problems using PBL, and to illustrate the inter-relationships between science, technology and human activity as it applies to digital forensics, forensic science and the criminal justice system. The paper concludes with an evaluation of the exercises considering the impact they have had on student understanding and learning. Consideration is given to how the PBL activities can be disseminated and/or transferred to the wider community.

KEYWORDS

Crime scene; search and seizure; problem-based learning

Introduction

The purpose of this paper is to compare and contrast the efforts of two universities to address the issue of providing computer forensics students with the opportunity to get involved in the practical aspects of forensic search and seizure procedures. Kerr (2011) indicates the importance of search and seizure in computer forensics, displaying the relationship between traditional forensic search and seizure process and procedures, but also recognising that there are important differences when dealing with digital evidence. Mason (2007, p. 249)

CONTACT Alastair Irons alastair.irons@sunderland.ac.uk

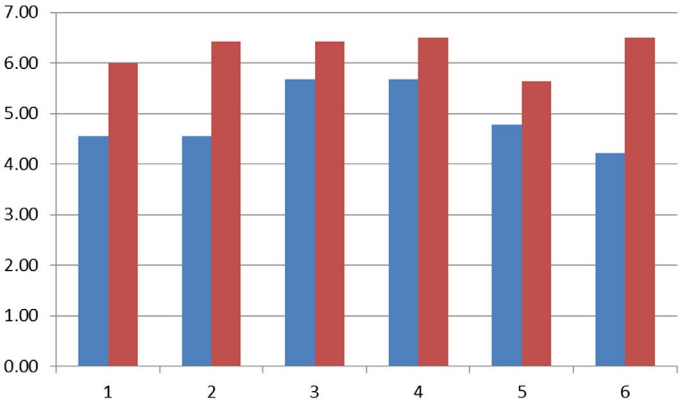

Figure 1. Student perception results 2013, data $N = 15$, pre $n = 8$, post $n = 14$.

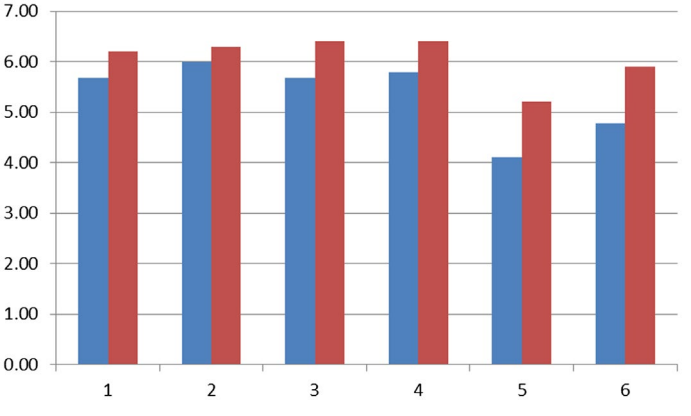

Figure 2. Student perception results 2014, data $N = 12$, pre $n = 8$, post $n = 10$.

argues that the search and seizure legislation in England and Wales 'undoubtedly cover the use of imaging technology to obtain copies of data held on a computer'. Rogers and Seigfried (2004) contend that the practical nature of computer forensics investigations pushes the teaching of computer forensics towards the more applied aspects of the discipline, and that this distorted focus is at the expense of the development of fundamental digital investigation theories. There have been examples in the past (e.g. Thurlby & Langensiepen, 2011) in using crime scene houses for computer forensics students – but the examples tend to focus on physical crime scene investigation using 'wet' forensics rather than computer forensics and digital evidence. For this paper, 'wet' forensics refers to traditional forensic science evidence, for example finger prints or sources of DNA such as hair samples.

Most computer forensic curriculum focus on teaching the correct procedures for imaging, analysing and reporting on digital evidence. These procedures are always based on the current Association of Chief Police Officers Good Practice Guide for Digital Evidence, ACPO (2011). These guidelines provide a benchmark for law enforcement and other practitioners to ensure that the digital evidence presented in a court of law has been correctly processed. They provide details of good practice for the complete process from the crime

scene through to the report of findings. Students of computer forensics are generally well versed in the ACPO guidelines as they are an integral part of their studies. However, they are rarely required to become familiar with guidelines relating to crime scene analysis as this aspect is often formally lectured with the student having little opportunity to gain any practical experience. Therefore, in order for a student to understand the complete forensic process, a practical understanding of the crime scene and its processing procedures is important. Many of these procedures have evolved in the practice of traditional forensic science and tend to be focussed on 'wet' forensics, however these practices are also relevant, and in some cases critical, to the correct processing of a digital crime scene.

This paper discusses the approaches undertaken by the University of Sunderland and the University of South Wales (Glamorgan) to give the students the opportunity to process a case from the crime scene through to the court room. In order to do this both institutions adopted a problem-based learning (PBL) approach – using problem scenarios to reflect real-world solutions and encouraging students to work in groups in order to work independently from tutors in seeking further knowledge and understanding of the various processes and procedures – in particular the steps around search and seizure of digital evidence from a crime scene.

Background to situation

Computer forensics students study a wide range of subjects including computer architecture, operating systems, programming and databases. This knowledge is required for the effective analysis of digital media which is the focus of most undergraduate computer forensics courses in the UK (Irons, Stephens, & Ferguson, 2009), and certainly is central to the computer forensics curriculum in both institutions in this study. Students gain experience of using a range of tools, both open source and proprietary, that are essential to the forensic analysis process. Understanding of the current guidelines and procedures is fundamental to this process as is the knowledge of legal requirements for digital-based evidence. As a result, computer forensics students are proficient at analysing the digital media, writing their results in the form of an expert witness report and then presenting their report in a mock court scenario. However, the initial part of the forensic process, the crime scene, is often overlooked in computer forensics course content or is discussed as part of the chain of custody and evidential integrity requirements and expectations of an investigation. There is usually little or no opportunity for students to gain experience of retrieving digital media from a crime scene. There are a number of reasons for this lack of content; for example it is difficult to create realistic evidence on digital media, there may not be an opportunity to include such practical content in the curriculum of such awards, or academic staff do not have access to items of digital media, practical support or the knowledge to develop such exercises. However, the main reason for not including such practical work is the lack of a crime scene. A digital crime scene can exist in practically any setting, for example a residence, an office, a street or a car. Digital crime scenes normally will include much more than digital evidence and will contain all the usual detritus of life, for example, a residence would contain furniture, personal items, clothes and all the items one would normally expect to find in a typical house or flat. Most academic institutions do not have access to such a facility, which is the main factor for the lack of crime scene content in computer forensic curriculum.

The computer forensics syllabus at both institutions is predominantly classroom based (theoretical and practical) and the search and seizure topics are embedded in the curriculum at various points throughout the programmes. The pedagogic approach adopted at both Sunderland and Glamorgan has always been to provide opportunities for putting theory into practice. The computer forensics content has evolved and become quite specialised. Students graduate with considerable knowledge of the analysis of digital media, the tools and techniques to be used and the writing and presenting of reports. They understand the forensic process from crime scene to court and the requirements of evidential continuity (chain of custody), but they have little or no experience of seizing and managing physical digital evidence. This is because most of their practical work is concerned with previously created digital forensic images and they have little opportunity to create their own images from digital media. In the past practical activities have been carried out by the use of digital forensic data-sets which have been created to give students the opportunity to get hands-on experience in the use of digital forensics tools and techniques. There are many practical activities included at both institutions but these tend to be very 'sanitised' – concentrating on the digital forensic recovery of evidence from PCs, discs, mobile phones etc.

Whilst the hands-on practical approach has proved popular with students and has enhanced learning, student feedback (from module review) indicated that they would improve their understanding of the digital forensic process if they had the chance to practise search and seizure processes and procedures, by providing a realistic environment to enable active learning about search and seizure. Feedback from students indicated that it is difficult for the students to visualise the context of the activities associated with a digital forensics crime scene, particularly the 'noise' involved in an investigation. In order to give students the chance to participate in active learning in digital crime scenes a PBL approach was developed to give students the opportunity to address the problems associated with digital investigations and collecting digital evidence from a crime scene.

Problem-based learning (PBL) has been used to positive effect in a number of academic disciplines; Boud and Feletti (1997, p. 1) advocate that PBL is the 'most significant innovation in education for the professions for many years'. PBL has been used in many disciplines including computer science for a number of years to develop students' skills in solving authentic and realistic problems. Discussion of PBL examples from the computing science literature include: Nuutila, Törmä, and Malmi (2005), Fee and Holland-Minkley (2010) and van Merriënboer (2013). Kessler (2007, p. 264) discusses the use of PBL in computer forensics problem solving:

> Ill-defined problems or scenarios can be a fun and interesting way for students to synthesize and/or expand their knowledge, making abstract concepts more real. In PBL problems and scenarios tend to be real, relevant, and tangible, students usually are more motivated to work hard on these projects, often making many real-world assumptions that are applicable to them, further helping to improve their problem solving skills.

Design of learning

The PBL activities at Sunderland and Glamorgan were designed in order to help the students understand the processes of digital crime scene analysis and search and seizure procedures and to give them the opportunity to put into practice their digital forensics techniques. Both exercises were designed to give the opportunity to solve realistic problems, using PBL, and

Table 1. Comparison of design of scene of crime activities.

	University of Sunderland	University of Glamorgan
Level of study	6	5
Summatively assessed	No	Yes
Location	Off site	On site
Forensic life cycle	Scenario planning, search and seizure, field image, transfer of artefacts	Scenario planning, search and seizure, field imaging, data analysis, report, mock court presentation
Use of PBL	Yes	Yes
Collaboration	With National Police College	With university's Forensic Science Department
Evaluation	Perception questionnaires	Summative performance

to illustrate the inter-relationships between science, technology and human activity as it applies to forensic science and the criminal justice system.

Table 1 compares and contrasts the design of the activities between the two universities. The activities at Sunderland were based around a set of formative exercises whilst the Glamorgan activities focussed on a 12-week exercise which was summatively assessed.

Case study 1 – Sunderland

The problem-based learning exercise(s) at Sunderland made use of the National Police Training College (NPTC) facilities at Harperly Hall. In order to address the request to facilitate search and seizure learning opportunities, discussions were held between the university and the NPTC to make use of the specialist training facilities – which include residential properties and a 'street' environment (housed inside a hanger) which has a number of commercial properties, the artefacts on a street (cars, dustbins, telephone boxes, etc.) and a number of bedsit properties. Collaborating with colleagues from the NPTC a scenario was created (see steps below) which demanded the gathering of digital evidence from the residential properties, the commercial properties and one of the bedsits. A physical and digital crime scene environment was created which had PCs, laptops, servers, routers and hidden CDs, USB sticks and floppy disks – and a shooting and a dead body!

The PBL exercise was spread over a number of weeks with the scenario given to students in stages. The students had to determine what it was that they needed to know and try to resolve a set of problems at each stage. The exercise started when the students were give a mobile phone which had an encrypted txt message (the txt message gave background to location and to a terrorist threat). The students then had to prepare for a potential search and seizure 'raid' – determining the equipment they would need, planning the pragmatics and obtaining appropriate search warrants.

The final stage before going to Harperly Hall was the provision of a brief – a 'physical' shooting (and resultant dead dummy body) had taken place and there were a number of digital artefacts at the scene with potential digital evidence on them (smartphone found on body, laptop in commercial property). Digital forensics specialists (the students) were required to do a search and seizure exercise and undertake field imaging of the artefacts where appropriate and/or bag and tag maintaining evidential integrity and continuity for transfer to the digital forensic lab at Sunderland for processing and analysis.

A day visit was arranged (the NPTC resource is located 30 miles from the university) for students. During the exercise the students were required to split into teams and were

required to plan, coordinate and manage the exercise. Students had a base room where they were expected to coordinate the search and seizure activities and the evidence collection. Students were given the opportunity to develop their team strategy for gathering digital evidence and were encouraged to consider other forensic issues (such as the need to involve other scene of crime colleagues for the gathering of 'wet' forensic evidence. Students had the opportunity to coordinate their activities and had a total of six hours to complete the search and seizure activities, the field imaging and the preparation of artefacts for transportation. The students were required to document all their activities.

In preparation for the exercise colleagues from the university collaborate with colleagues from the NPTC to set up the scenes of crime and establish the digital evidence. Simple, but context specific, digital evidence data-sets were created and placed on a variety of digital devices. The digital evidence was obfuscated with large amounts of digital data to act as noise. Devices were located in commercial premises on the street – near the 'shooting' and at the nearby residential premises (the crime scene house) – which meant that the students had to split their team resources to cover multiple crime scenes.

The students were given the full responsibility for determining their course of actions, their search and seizure protocols, their field imaging strategies, the documentation of their activities and the preparation for transportation of all seized artefacts back to Sunderland.

Case study 2 – Glamorgan

The activities at Glamorgan were designed in collaboration with the Forensics Science Department. The activities centred on a large assessment exercise over a 12-week period that included the analysis of digital evidence in the form of a previously created forensic image and then producing the report for court. The students worked in groups for this exercise. The students were required to observe ACPO guidelines for chain of custody, evidential integrity and to create their own forensic image of the digital media retrieved. The activities took place in the University of South Wales' own scene of crime house, which is a three-bedroomed detached house located on campus. The house is fully furnished and contains a wide range of other items like clothing, kitchen items, etc. There are also a number of realistic dummies which occupy the house and have evidence of physical harm. The injuries vary depending upon the current theme of the forensic science assessments. The Computer Forensics team were able to make use of the resource on the condition that they did not tamper with any of the existing contents.

This activity required considerable planning as a number of elements had to be in place for the practical exercise. These elements were the availability of the crime scene house, the scenario, the digital media containing evidence items and the skills of the students. The crime scene house was heavily timetabled for forensic science activities so the activity had to take place when there was some free time. A four-hour afternoon slot was offered which would limit the time the students could have in the house. Ideally a full day would have been preferable as then each group could have enough time to process the entire house rather than just a couple of rooms. The amount of digital media from the house had to be retrieved within a shorter time slot and therefore the amount of digital media items was reduced.

The scenario was developed with the suspect living at the crime scene house with his mother; however the suspect was identified as having recently left the area due to law enforcement interest. The aim of the scenario was to present the students with a realistic

Table 2. Categorisations used in student perception questionnaire.

	Category
1	Digital forensics in general
2	Search and seizure processes and procedures
3	Evidential integrity
4	Evidential continuity (chain of custody)
5	Field forensics procedures
6	Professional practice

Note: The data were gathered and collated for the 2013 and 2014 cohort – see Figures 1 and 2.

experience of investigating a crime and therefore the evidence items and digital media had to be appropriate. The basic scenario was the same but each group of students was allocated a different crime – drug dealing, illegal downloads, distribution of child pornography and blackmailing local businesses. Each crime needed to have appropriate items of evidence, the same digital media, require similar processing time and use the same tools and techniques for analysis. This was to ensure that each group of students had a comparable experience and that there was no variation in the assessment content.

A number of digital media items were considered for the assessment. There were concerns regarding the amount of time that it would take to image and analyse a typical laptop due to the size of the hard drive. The creation of the evidence items on a forensically 'clean' device was also a consideration as developing evidence items and 'noise' content over a timeline can be rather intensive. It was therefore decided to use smaller, more manageable digital media, meaning each scenario had evidence items placed on one mobile phone, one USB flash drive and two CD-ROMs.

It was also identified that some additional personnel would be required to help with the organisation and running of the activity on the day. As the students were being assessed on their processing of the crime scene there need to be observers in each room in the house. The evidence items would need to be 'hidden' prior to each group's time slot so this task could be allocated to the observers. Each group of students would need to sign for appropriate items of clothing i.e. overalls, gloves, overshoes and mask, so an additional room was required with personnel to monitor the clothing allocation.

The activity took place during an afternoon when the crime scene house was available. There were eight groups of students who needed to process the crime scene during the four-hour slot, therefore each group was scheduled a 30-min time slot. Prior to the activity, each observer was given the digital media for each scenario and the assessment marking sheets. The observers were each allocated a room in the house and were responsible for 'hiding' the digital media in their room and marking the students on their crime scene processing activities.

Each group of students arrived at the crime scene house and had to present their search warrant to the Officer in Charge who was in the house. They were then permitted entry and their processing could begin. A range of evidence bags were placed in the hallway for the students to use. They were assessed by the observers on the way they handled the digital evidence, the recording of the evidence items and their crime scene processing skills.

Each group was responsible for the digital media they had retrieved as these items would need to be imaged and forensically analysed in order to produce the expert report. The transportation of the digital media from the crime scene and its secure storage was the responsibility of each group.

Table 3. Comparison of summative performance between 2013 and 2014.

	<40	40–49	50–59	60–69	70+	No in cohort	Ave	SD
2013	2%	9%	31%	44%	13%	45	59.28	10.41
2014	0%	0%	6%	68%	29%	31	66.94	5.27

Methodology and analysis

The two universities used a different approach in gathering data about the activities, but both used a framework of trying to obtain a measure before the event and then after. In the case of Sunderland where the activity has happened on two separate occasions with two different cohorts a pre- and post-questionnaire was used to obtain students perceptions on the categories indicated in Table 2 using a scoring system of 1–8 where 1 = not confident and 8 = very confident.

The responses were averaged in each category and provided interesting reflection on the students' perception of improvement of understanding across the range of categories in each cohort. It was noticeable that the increase in perception levels was more marked in the first cohort than the second. Further analysis work is underway looking at the improvements at individual student level, and that data will be presented at a later date.

The Glamorgan analysis is based on improved performance on summative assessment comparing two cohorts – the 2013 cohort did not have the crime scene PBL exercises and the 2014 cohort did, see Table 3.

The improvement in student performance at Glamorgan can be attributed to the more complete PBL exercise which had a series of submission milestones during the spring term, although it is recognised that other variables such as cohort ability and experience, teaching and emphasis of the subject matter also potentially contribute to the improved summative performance. The students had to take responsibility for the digital evidence retrieved from the crime scene as these items would form the basis of their case and subsequent assessment. Therefore, they developed a sense of ownership of the case and wanted to process the digital evidence to the best of their ability. They were very cautious in the procedures they used to image the digital evidence and were extremely concerned about preventing contamination of the evidence items. This resulted in activities being planned in advance and detailed notes maintained. Overall, the increased attention to detail, the observation of guidelines and more complete documentation resulted in improved marks.

Reflection on the activities

Both institutions organised the students into groups for the practical PBL crime scene analysis. This gave the students an opportunity to work as a team and to organise their activities accordingly in their attempts to solve problems. The group activity gave the students confidence during the practical crime scene analysis as they were not working alone and had their peers to support them. Some groups were better organised than others and this was reflected in their feedback and practical assessment.

In both institutions students had the opportunity to provide feedback after completing the activities. A number of comments reflected the reaction from students, e.g. 'Didn't realise imaging would be so stressful', but the majority of comments were positive. The following list provides typical examples:

Good to have hands on experience at an actual crime scene.

Need to be fully prepared before entering a crime scene.

Understood why professional responsibility is important.

Can we do it again please?

However, at both institutions there was a common complaint that the students did not have enough time at the crime scene to process the crime scene thoroughly. This was partly due to the way they had organised themselves while at the crime scenes and partly due to the limited time periods allocated to carry out the crime tasks. Some groups had already discussed how they were going to approach the processing of the crime scene and allocated resources appropriately, which was an effective way of getting the work completed. At both institutions there were instances when students did not follow the plans and as a result tended to wander around the crime scenes at random and then ran out of time and sometimes failed to locate all the evidence items.

At Glamorgan the students disliked the observers in the rooms of the house as they felt they were being watched; which they were. However, the observers were consistent in their marking and also provided valuable verbal feedback on each group's activities in the house. Sunderland did not make use of observers.

At both institutions the need for search warrants proved to be useful in giving the students an insight into the legal requirements of crime scene processing and having a colleague pose as the Officer in Charge gave the activity some gravity. The groups were not permitted to enter the crime scenes until the Officer in Charge had verified their search warrant.

The recording of the digital media items retrieved and the completion of the evidence bags details varied between groups. Not all groups completed the details when each item was retrieved due to lack of time and the naming conventions used were irregular on occasions.

Providing crime scene clothing was very effective and all the students enjoyed getting 'dressed up' for the activities. There were many 'selfies' and group photographs on social media, although getting into and out of SOCA suits proved difficult for some students.

The examples discussed in this paper show how the integration of problem-based learning into the computer forensics curriculum can enhance the students' understanding of digital forensics principles and protocols. By developing PBL activities which are fun and interesting for students to participate in the students will be more motivated to participate in the activities and as a result expand their knowledge and understanding. The use of realistic settings and the combination of physical and digital crime scenes help to make abstract concepts more real for students.

One of the major challenges in teaching computer forensics is the development of case material, examples and digital evidence data-sets. One of the problems facing the computer forensics teaching community is the duplication of effort across different institutions. There is a willingness to share materials as evidence in previous Higher Education Academy Teaching Computer Forensics Workshops, however there is a need to consistently update and develop these materials in order to provide problem solving opportunities for students. If the data-sets are not refreshed and kept up to date then the data-sets become unsuitable for use in summative assessments, the students can potentially find solutions online and cease to be challenged (Tryfonas, 2008) or the challenges don't keep up with technology and become less motivating for students (Lallie, 2010). It is anticipated that the scenarios that have been

developed at Sunderland and Glamorgan will be transferable to other institutions – albeit with the proviso that suitable physical crime scene resources are taken into account.

Conclusions and further work

Overall, the activities at both institutions were extremely successful and provided the students with an excellent experience. The students were nervous prior to entering the crime scenes as they were not given access prior to the facilities. This meant they had no idea what they were going to encounter. The crime scene facilities whilst being 'set up' are also deliberately kept rather untidy, cold and scruffy. There were dummy bodies that had been placed around the crime scenes and some of these had suffered terminal injuries. The students found these bodies a distraction and a bit disturbing. However, the students were very positive in their feedback and offered to help as observers for the activity next year.

At Glamorgan the main change for the next academic year will be an increase in the amount of time that each group has in the house and to allocate certain rooms to each group rather than the entire house. This will enable the students to thoroughly process the crime scene and to adhere to the guidelines more effectively. It is anticipated that each group will be allocated 45 min, but have only two rooms to process.

At Sunderland the main change for next year will be to have an even more authentic scenario to give the students a bigger and more effectively interrelated and more complex problem to solve. To this end academic colleagues and students from the university's creative writing department are collaborating with the computer forensics team to make a better story.

The activities at Sunderland and Glamorgan have demonstrated that students lack the knowledge and skill to process a crime scene, but by utilising PBL they learn from the opportunity to practise the skills and techniques of search and seizing digital evidence. Students need to understand how digital evidence is retrieved and the importance of evidential continuity and integrity and undertaking a practical activity like this provides them with this knowledge. Most computer forensic practitioners never visit a crime scene and therefore it should not be a significant part of a computer forensic award, however, it is a valuable skill that can be achieved through practical activity.

References

ACPO. (2011). *Good practice guide for computer-based evidence*. Retrieved June, 2014, from www.acpo.police.uk/documents/.../201110-cba-digital-evidence-v5.pdf

Boud, D., & Feletti, G. (1997). *The challenges of problem based learning*. London: Kogan Page.

Fee, S.B., & Holland-Minkley, A.M. (2010). Teaching computer science through problems, not solutions. *Computer Science Education, 20*, 129–144.

Irons, A.D., Stephens, P., & Ferguson, R.I. (2009). Digital investigation as a distinct discipline: A pedagogic perspective. *Digital Investigation, 6*, 82–90.

Kerr, O.S. (2011, November 19). Searches and seizures in a digital world. *Harvard Law Review*, Vol. 119, p. 531, 2005; GWU Law School Public Law Research Paper No. 135. Retrieved June 1, 2014, from SSRN: http://ssrn.com/abstract=697541

Kessler, G.C. (2007). Online education in computer and digital forensics: A case study. In *IEEE Proceedings of the 40th Hawaii International Conference on System Sciences 2007*. Honolulu.

Lallie, H.S. (2010). Developing usable hard disk images for forensic training, education and research. In *4th International Conference on Cybercrime Forensics Education and Training 2010*. Canterbury: Canterbury Christchurch University.

Mason, S. (2007). England and Wales. In S. Mason (Ed.), *Electronic evidence, disclosure, discovery and admissibility* (pp. 175–282). London: Lexis Nexis, Butterworths.

Nuutila, E., Törmä, S., & Malmi, L. (2005). PBL and computer programming — The seven steps method with adaptations. *Computer Science Education, 15*, 123–142.

Rogers, M.K., & Seigfried, K. (2004). The future of computer forensics: A needs analysis survey. *Computers and Security, 23*, 12–16.

Thurlby, C. & Langensiepen, C. (2011, November). *Use of a crime scene house to facilitate learning*. Paper presented at Higher Education Academy 7th Teaching Computer Forensics Workshop, Sunderland. Retrieved June 1, 2014, from http://www.ics.heacademy.ac.uk/events/displayevent.php?id=264

Tryfonas, T. (2008). *Developing learning resources for the tuition of computer forensics*. In HEA Information & Computer Sciences Subject Centre Annual Conference – HEA-ICS, Liverpool Hope University, Liverpool.

van Merriënboer, J. (2013). Perspectives on problem solving and instruction. *Computers and Education, 64*, 153–160.