THE USE OF SIMULATION IN DIGITAL FORENSICS TEACHING

Jonathan Crellin
School of Computing, University of Portsmouth
Buckingham Building
Portsmouth, PO1 3HE
jonathan.crellin@port.ac.uk

http://userweb.port.ac.uk/~crellinj/indexd.php

Mo Adda
Mo Adda
School of Computing, University of Portsmouth
Buckingham Building
Portsmouth, PO1 3HE
mo.adda@port.ac.uk

Emma Duke-Williams
Emma Duke-Williams
School of Computing, University of Portsmouth
Buckingham Building
Portsmouth, PO1 3HE
emma.duke-williams@port.ac.uk
http://userweb.port.ac.uk/~duke-wie/blog/

ABSTRACT

Simulation at different levels of fidelity has been used in education and training for many years. This paper will look at the use of simulation in this area of Computer Science education, and reports on a number of different simulation tools in use in the University of Portsmouth. Central to digital forensics education is a life cycle that involves forensically safe seizure of digital evidence, imaging of digital devices, their investigation, report writing, and acting as an expert witness in court. Several of these activities are suitable for simulation based education. In teaching of digital forensics at the University of Portsmouth simulation of forensically safe seizure has used simulation. This usually involves constructing a scenario where a running computer is seized and imaged, which involves using an office like room, and providing a computer that has been suitably prepared. Many universities now have 'forensic houses' which are simulated crime scenes, that are used to support a variety of forensic disciplines, and these can provide a suitable context for seizure simulations. The University of Portsmouth has operated a forensic house for about five years. Another area of simulation is in court room work. Many digital forensic specialists will be required to give evidence in court at some stage of their career. Again, a number of universities have set up simulated court rooms, and the University of Portsmouth opened its crown court room simulation in February 2010. The simulated court room is a room laid out as a crown court, with video recording facilities, and external features such as jury rooms, interview rooms and facilities to support the giving of video evidence. This year the digital forensic students were required to give evidence in this court as part of their assessment. Although the court was not fully simulated (only roles of defence and prosecution council, judge, usher, and accused were represented) the experience was reported by students as being quite intense.

The benefits brought to the unit by simulation were mainly in terms of increasing enjoyment and motivation among the students. All the staff involved in the teaching were surprised by the almost ecstatic reaction of many students on the unit to the simulation experience. The main disadvantages were the costs involved in setting up simulations, which are quite high, especially for the seizure simulation. Also for individual simulation the time involved was high. For example the court simulation required each student to give evidence independently, and be cross examined, even with a small MSc class this took nearly three hours. Seizure simulation involved team work, with only one student actually directly performing the seizure (under direction from her peers).

In 2009-2010 we have investigated the use of virtual world simulations for digital seizure, constructing a number of test examples (with the help of students studying an interaction design unit). These potentially allow a low cost replaying of seizure scenarios, allowing individual students to experience different scenarios on demand. A similar opportunity exists for familiarisation with court room procedure. We will evaluate these low fidelity simulations with students in 2010-2011.

Keywords

simulation, digital forensics, teaching, virtual worlds

Subject Centre for Information and Computer Sciences

1. INTRODUCTION

1.1 Simulation in computer science teaching

Simulation forms a important part of many aspects of computer science teaching. It covers low fidelity simulation (for example the specification for a programming task) to high fidelity simulation (for example requirements capture from staff simulating business roles for system analysis). Simulation has two important aspects. The first is that at least one important aspect of the target context is accurately mimicked, and second that it is safe, the participant cannot suffer any significant damage (but may experience some of the emotions or challenges of the real situation). A flight simulator recreates the changes in force as an aircraft changes orientation and speed, the appearance of the ground from the cockpit, and the controls available in the aircraft. But a flight simulator is safe. Although the simulated aircraft may crash, the physical forces experienced by the participant will never be dangerous. The emotional experience may be intense. Simulations form one important class of game (either in a computer simulation, or in a realistic role play) because of the opportunity to experience intense emotions in a safe context.

This safe experience of dangerous contexts also allows for education and training. Flight simulators have been used since the early twentieth century to introduce trainee pilots to the difficult aspects of flying without putting the trainees at risk (Link Simulator, L-3 Communications, 2009). In more 'academic' domains, simulations may be used in operating theatre, or intensive care ward practice (ExPERT Centre, 2008), and virtual worlds have been used in computer science education in a number of ways (Crellin, Chandler, Duke-Williams, & Collinson, 2009).

1.2 Digital forensics investigation lifecycle

Central to digital forensics education is a life cycle that involves four main steps. The first is the forensically safe seizure of digital evidence. This means data stored on a variety of devices, typically computer hard disks, or flash memory devices. Increasingly mobile devices are important for investigation. The core principal of any forensic investigation is that the process of collecting evidence must not change the evidence in any way. Where evidence is in a dynamic state (for example data on a running computer) the seizure process is more complicated. The Association of Chief Police Officers (ACPO, undated) defined a process for forensically safe seizure of evidence, and whilst this is becoming less appropriate as computer systems evolve (particularly the increased use of disk encryption), it does provide a baseline for approaching the problem.

Once collected devices must be examined and analysed. This usually involves looking for particular data on the device. The data is often hidden, and novice investigators will need to undertake a number of investigations of increasing complexity in order to acquire the necessary skills. The provenance of the material found is as important as it presence. The investigation process is reported in detail, as well as the findings.

A court report will detail the findings, and the process in a replicable form, since expert witnesses working for the defence may wish to critically evaluate the investigation process.

Finally an expert witness will give evidence in court. In a Crown Court, evidence is given to the judge and jury, but is elicited through questions from council for defence and prosecution. Hence the expert witness cannot usually make a presentation to the judge and jury, but must rely on the questions of council to elicit the key points of evidence. It is a strange and artificial process, and one that requires quick reactions to the opportunities presented by the questions.

2. USE OF SIMULATION IN OUR TEACHING OF FORENSICS

2.1 Seizure simulations

A seizure simulation involves presenting students with a simulated environment which contains data devices of one sort or another, with the challenge that these be collected in a forensically safe way. In practice digital forensic specialists may not be present at the scene, however they may be called in to deal with evidence that scene of crime officers cannot deal with. One example might be a running computer. A running computer provides several challenges. Closing a computer down may inadvertently lead to loss of evidence (and the computer may be designed to remove incriminating evidence under some circumstances). Closing a computer down normally will produce a great deal of disk activity, with access and updates to many files. In some cases a running computer may provide the best opportunity for accessing concealed or encrypted files. A computer is also a communications device and a running computer may be connected to a site of interest to the investigator.

In our simulation a room will contain a running PC. Normally some contextual evidence will also be available. Students' task is to decide the best way to close down the computer, and dismantle it for evidence collection. We usually allow one student to act as the evidence collection officer, and the others to direct, take notes and discuss the courses of action available. We have typically included 'surprises' based on reports from our professional advisors which usually add to students engagement with the simulation.

Students finally image the hard drive that they have extracted during the simulation, and this image is then used during their assessment.

Setting up this type of scenario can take some time, usually getting a small room that is not obviously a classroom can be difficult. A computer needs to be set up, a variety of additional elements need to be used to 'dress' the scenario. Various consumables such as latex gloves, evidence bags etc. are needed, and various pieces of specialist equipment (write blockers etc.) have to be brought in. The costs are small, but even a simple simulation needs an hour for preparation and an hour for dismantling.

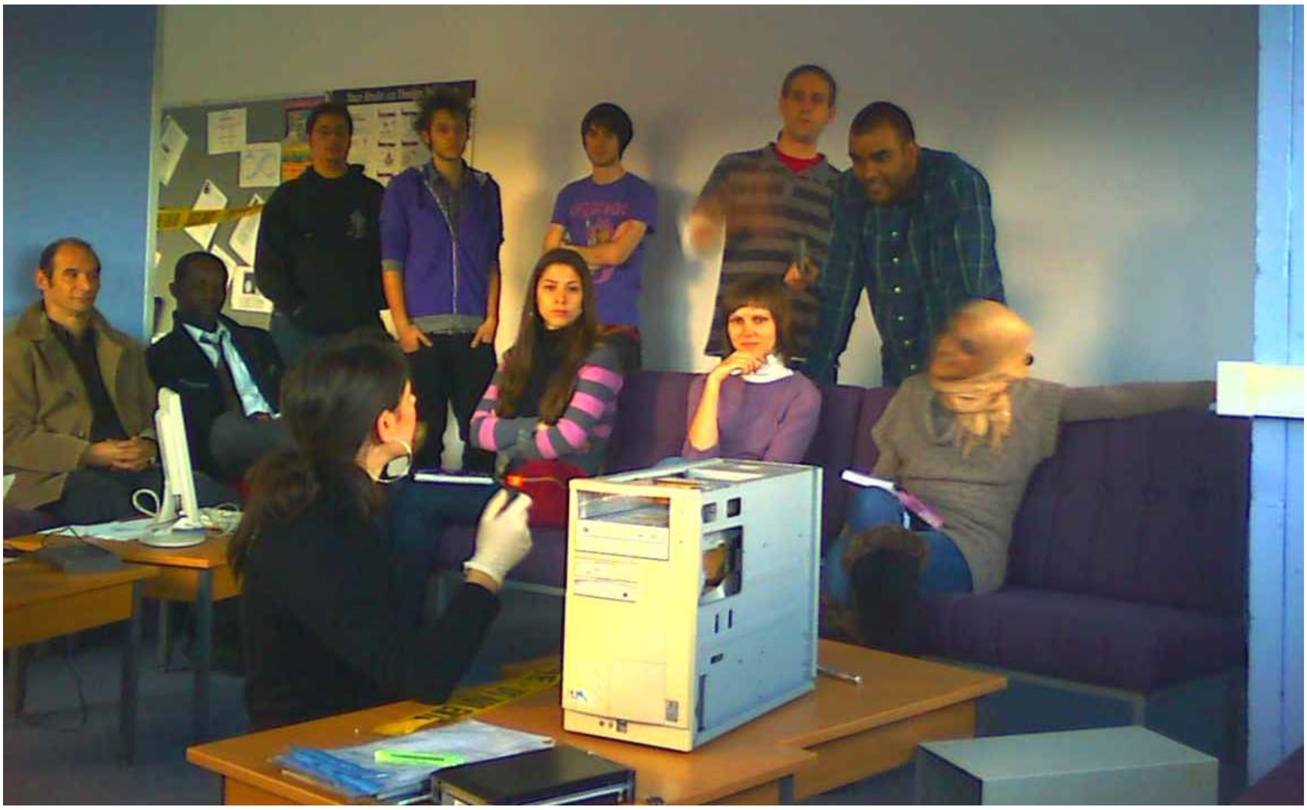

Fig1: Seizure Scenario demonstrating team based work. With one student performing the majority of the hands on work whilst others direct, discuss, comment and record the process.

2.2 Court room simulations

A second area of simulation is in court room work. Many digital forensic specialists will be required to give evidence in court at some stage of their career. Again, a number of universities have set up simulated court rooms, and the University of Portsmouth opened its crown court room simulation in February 2010. The simulated court room is a room laid out as a crown court, with video recording facilities, and external features such as jury rooms, interview rooms and facilities to support the giving of video evidence. This year the digital forensic students were required to give evidence in this court as part of their assessment.

The simulation involved a mock court room, and ancillary rooms (interview rooms, a witness waiting room, and a jury room) that has been built in the University, with several members of staff playing critical roles. The simulation was of a Crown Court. A member of staff with some prior experience played the role of judge, the two unit lecturers played the roles of defence and prosecution council, an unfortunate pair of research students played the defendant and his guard (largely passive roles), finally another student played the role of court usher, bring the forensics students playing expert witness to and from the court room. Each student was allowed to stay in the public gallery to see the following expert witness. The mock court room has been equipped for video recording, however the new equipment did not work correctly (having just been set up) and so we didn't have the opportunity to use the footage in review with students.

The context, and simulated formality of the environment greatly affected the students, who found the experience fairly intense. Although we had originally considered using strangers as council, having familiar lecturers (albeit somewhat oddly dressed) was probably beneficial in moderating the stress of the simulation.

The setup of the court was fairly minimal as it is a ready dressed set. Only some additional props, oath cards, information typically provided by courts to witnesses, were required. Running the simulation involved repeatedly questioning and cross examining each student. The performance of students under cross examination was rated by the two unit lecturers, and formed one element of the assessment mark. The court report was also submitted for assessment. The main costs of the simulation were staff time, and the time and availability of the people who played the additional roles.

2.3 Virtual world simulations

Using HCI undergraduate students a number of simulated environments were set up, using the virtual world Second Life, which is relatively accessible (Linden Research Inc., 2009). These environments were incomplete but did demonstrate a number of different approaches that could be employed. In such a virtual world the behaviour of seized devices can be closely simulated, by feeding output from virtual machines running outside the simulation. Conventional approaches to seizure (as described by ACPO) as well as contemporary approaches (memory capture) can be attempted. The approach was discussed in (Crellin and Karatzouni, 2009).

In 2009-2010 we have investigated the use of virtual world simulations for digital seizure, constructing a number of test examples (with the help of students studying an interaction design unit). One example is shown in figure 2. These potentially allow a low cost replaying of seizure scenarios, allowing individual students to experience different scenarios on demand, and replaying them on demand, without a tutor necessarily being present. We will evaluate these low fidelity simulations with students in 2010-2011, and contrast the different levels of fidelity involved.

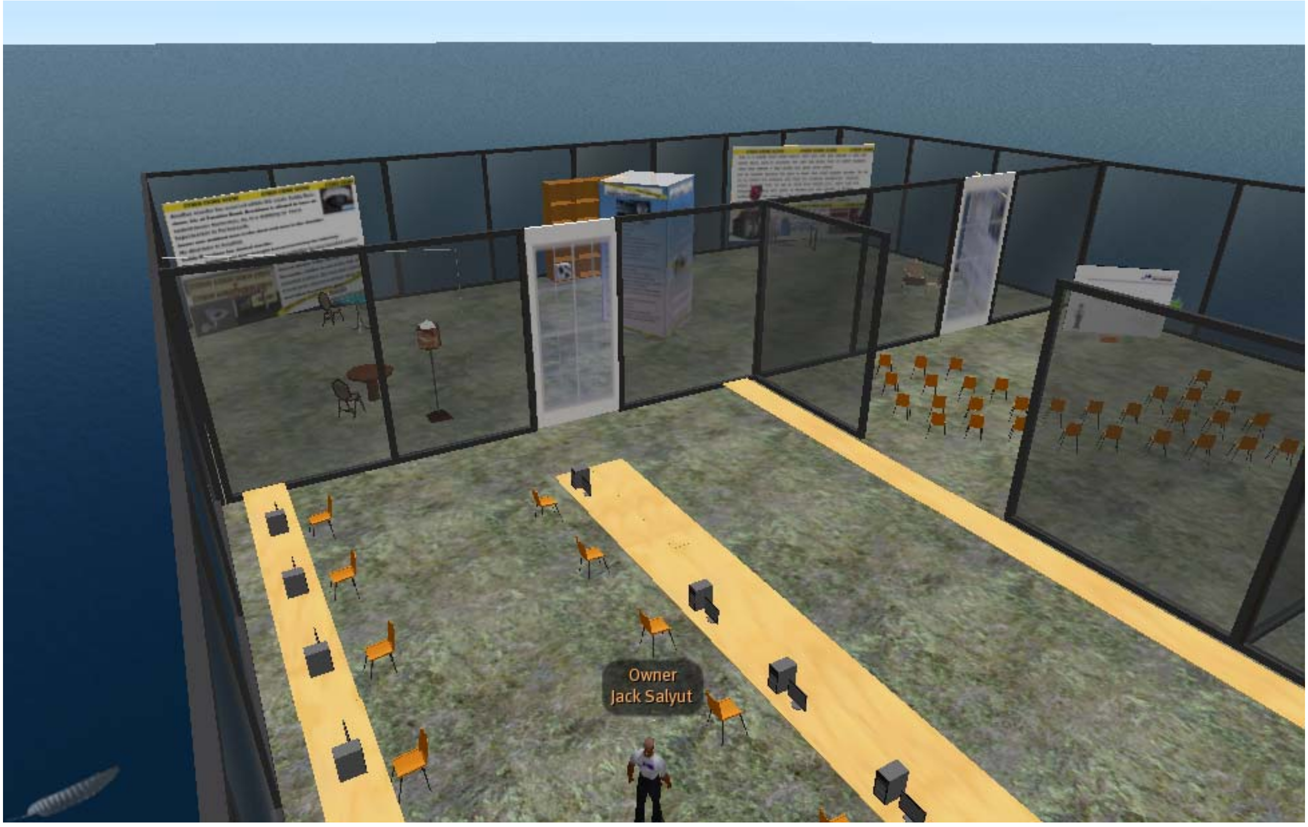

Fig2: One example of a virtual seizure simulation environment in Second Life. The environment includes learning material in one bay, a simulation exercise in the second bay, and assessment exercises in the third bay. As a stand alone environment students could use it at any time, presence of a tutor is optional.

2.4 The forensic house

Many universities now have a 'Forensic House' which are simulated crime scenes, that are used to support a variety of forensic disciplines, and these can provide a suitable context for seizure simulations. The University of Portsmouth has operated a forensic house for about five years. This environment will usually represent a domestic context with evidence of a crime, for example blood stains, evidence of a fight etc.. The forensic house can provide a good environment for running a seizure simulation, although digital forensic officers would not often operate in the scene of crime.

3. IMPACT ON STUDENTS

The use of simulation was extended in 2009-10 with the first use of the mock court room. Contrasted with a functionally similar assessment viva in 2008-9, the simulated court room appears to be much more engaging for students. A seizure scenario had been used in 2008-9 successfully and the response of student in 2009-10 was also very positive. The unit received the highest feedback ratings of any post-graduate unit, and second highest of any unit taught by the School of Computing. Qualitative feedback suggested that the seizure simulation had been the most appreciated part of the unit.

Student understanding may not be enhanced greatly by the use of simulation. Performance on the assessments varied across the class, and some obvious points made in the simulation were missed by some students.

4. SUMMARY AND DISCUSSION

Simulations do enhance student engagement with the unit. The benefits brought to the unit by simulation were mainly in terms of increasing enjoyment and motivation among the students. All the staff involved in the teaching were surprised by the almost ecstatic reaction of many students on the unit to the simulation experience. Its less clear if they enhance cognitive skills, but they do help replicate some of the emotional pressures involved in the subject area. The principle disadvantage of simulation is the cost of setting up the environment. This includes equipment costs, which may be quite low (given that some items will usually be little more than standard piece of equipment) but will include consumables. The larger cost is the time to set up environments, even if a custom environment is available it usually still needs some dressing. Computers need to be re-imaged, set up in the environment. Often quite heavy items moved from one location to another. Several participants will need to play specific roles, especially for court room simulations. A degree of acting is necessary. Time for running even fairly small scale simulations is quite long. The main disadvantages were the costs involved in setting up simulations, which are quite high, especially for the seizure simulation. Also for individual simulation the time involved was high. For example the court simulation required each student to give evidence independently, and be cross examined, even with a small MSc class this took nearly three hours.

Integrated simulations across faculty appear possible, and very interesting, but even more difficult to run. They need to meet the varied assessment requirements of different disciplines, course timetables, and the need to co-ordinate a larger number of students and classes. In such a cross faculty simulation law students may take on court roles, and different forms of forensic evidence might be presented, for example physical evidence collected in the forensic house, alongside digital forensic evidence, and forensic accountancy may all be components in a simulated court case.

Using simulation in teaching can be very effective with students, and very rewarding for teachers, but one should never underestimate how important staff enthusiasm is for a successful simulation.

5. REFERENCES

Association of Chief Police Officers of England (ACPO) (undated) Good Practice Guide for Computer Based Evidence http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf (accessed 21-May-2010)

Crellin, J., Chandler, J., Duke-Williams, E. and Collinson, T. (2009) *Virtual worlds in computing education*, Computer Science Education, Vol. 19, No. 4, December 2009, 315–334

Crellin, J., Karatzouni, S. (2009) Simulation in digital forensic education, at the 3rd International Conference on Cybercrime Forensic Education and Training (CFET3) (BCS SIG) Conference, Canterbury Christ Church University, 1st - 2nd September 2009.

L-3 Communications (2009) *Link Simulation & Training: Setting the standard for 80 years* http://www.link.com/history.html (accessed 23-August-2009)

Linden Research Inc. (2009). Linden Lab. from http://lindenlab.com/ (Accessed 20-August-2009), Reynolds, L, (2007) HEFCE Evaluation ExPERT Centre 2005-2007, from: http://www.expert.port.ac.uk/assets/documents/WEBv%20Evaluation%202005-07.pdf (Accessed 15-August-2009)