Simulation in Computer Forensics Teaching: the student experience

Jonathan Crellin[1], Mo Adda[2], Emma Duke-Williams[3], Jane Chandler[4]

[1,2,3]School of Computing
University of Portsmouth
Buckingham Building
Lion Terrace
Portsmouth
PO1 3HE
[1]jonathan.crellin@port.ac.uk
[2]mo.adda@port.ac.uk
[3]emma.duke-williams@port.ac.uk

[4]Faculty of Creative & Cultural Industries,
University of Portsmouth,
7th Floor,
Mercantile House,
Hampshire Terrace,
Portsmouth,
Hampshire, P01 2EG
jane.chandler@port.ac.uk

Keywords: Computer Forensics, Virtual Worlds, simulation

Abstract
The use of simulation in teaching computing is well established, with digital forensic investigation being a subject area where the range of simulation required is both wide and varied demanding a corresponding breadth of fidelity

Each type of simulation can be complex and expensive to set up resulting in students having only limited opportunities to participate and learn from the simulation. For example students' participation in mock trials in the University mock courtroom or in simulations of digital seizure in the University Forensics House require many months planning and co-ordination across Faculties. To enable students to gain more experience, in a cost effective way, simulations are being developed in Second Life to for seizure of digital evidence and to provide opportunities for students to practice as expert witnesses in a virtual courtroom.

Examples of the simulation techniques and of student use are described and include for examples of: simulated seizure of evidence; simulated case investigation; investigation techniques that involve virtual simulation of systems; simulated court appearances (for example as expert witnesses).

Student feedback suggests that simulation is usually highly appreciated by students, but also can induce stress and anxiety in some instances. This paper reviews evidence from students, qualitative and quantitative, and discusses the pros and cons of simulation for both teachers and students.

Simulation in teaching and training

Simulation has been used in many areas of educational and training. In the twentieth century increasing complex technology was used to create higher fidelity simulations. In the area of pilot training, where the underlying activity is always dangerous, flight simulation began within a few decades of the first manned flights, with, for example, the Link simulators providing an increasingly complex series of flight control simulators (L-3 Communications, 2009).

Simulation has also been used in training social skills. For example training a candidate (or interviewer) involves simulating an interview and then reviewing recordings of the interview after the event. A similar approach is used in systems analysis and design, where participants playing the key business roles are interviewed by teams of students in order to gather data about system requirements (Zowghi & Paryani, 2003).

There are a number of areas of digital forensics teaching that suit a simulation approach. In practice most digital forensics units make use of a problem solving pedagogy, and often involve students working on a case. Digital forensics involves a three stage process, beginning with the acquisition of digital evidence (sometimes referred to as seizure), the analysis of digital evidence (often surprisingly complex due to the huge number of files found in all modern operating systems), and the presentation of evidence to laymen (for example to a lay jury).

Digital Forensics Simulations

Seizure

Seizure is the process of seizing the information system from a crime scene or suspect. As with any forensic evidence it is vitally important that evidence is not changed by virtue of the process by which it is obtained. Conventional forensics scientists will wear sealed clothing in order to minimise contamination of a crime scene, and will ensure that each item of evidence is collected in a way that prevents transfer of (e.g. fingerprints or DNA) from the forensics officer to the evidence.

Digital evidence can be somewhat different. A running computing will usually be running processes all the time. The action of shutting down a computer operating system will involve many operations, data being written to log files, files being closed and deleted, updated modification dates etc. It therefore becomes very difficult to demonstrate that intentional changes have not occurred to a piece of digital evidence. Most police services around the world have issued guidelines about the methods that should be used to secure digital evidence. In the past failure to secure digital evidence has cast doubt on the validity of the evidence, and its validity has been open to question. For example in the Julie Amero case (Losavioet al 2008) highlighted the difficulties the legal profession has with digital forensic evidence when a high school teacher was accused of showing her students pornography. The case revolved around the use of unwanted 'pop up' images, and whether these were triggered by the accused or whether the images were due to malware.

In the UK the Association of Chief Police Officers provides a document that advises on a legally and forensically safe digital seizure procedure (ACPO, 2007). Unfortunately general guidelines may not be useful due to the possibility that a computer may be running one of a variety of operating systems and may have one of a variety of disk encryption systems installed. The traditional process of disconnecting the power supply and removing hard drives is less appropriate when that might simply capture highly encrypted data that is (for all intents and purposes) unrecoverable without the co-operation of the suspect. In addition changes in technology mean that the procedures followed have to continually adapt. Students need to be able to make appropriate judgements about the seizure process to undertake, so that they have the best chance to circumvent any 'anti-forensic' strategy undertaken by a suspect.

Seizure simulations usually involve presenting students with a running computer in an office like environment (often a staff office or similar). Students are then asked to perform a seizure. Such simulations are usually quite engaging for the students but do involve quite a lot of preparation, and often involve one student acting as an 'avatar' for a whole class (Fig 1).

Fig. 1 Seizure Scenario demonstrating team based work: one student performs the majority of the hands-on work whilst others direct, discuss, comment and record the process.

After seizure and imaging students will end up with a disk image. This image is a bit copy of the computer's hard drive, and it is this which they preserve and analyse, looking for evidence. Constructing meaningful cases is often one of the most difficult parts of teaching digital forensics, since it is necessary to create a 'trail' of events on the hard drive which are consistent with the criminal and innocent behaviour of the suspect. Virtual computer systems are used to construct these cases, and may also be used by analysts to get a 'suspect's eye view' of the system being examined. A range of commercial and freely available tools can be used for virtualisation.

However the legal forensic evidence is usually the result of analysis of images using specialist software, widely accepted as legally sound. In this way files and records of interest may be discovered and these will usually form the basis of a digital forensic expert's report.

Court rooms and giving evidence

Giving evidence as an expert witness is something that many forensics experts may be required to do during their career. Expert witnesses usually have to explain the evidence and its meaning to a lay jury. For digital forensics experts the evidence may involve complex and counter intuitive concepts. For example an explanation of why a digital photograph file, appearing on a computer, may never have been actually seen by the user of the computer. The usual process for an expert witness is to write a detailed report (which must follow certain guidelines, and must not itself break the law), and then to be examined and cross-examined by council for defence and prosecution, in court. The basic process of being a witness is straightforward, but can be very intimidating and stressful. Expert witness may be called to a number of different types of court.

During digital forensics courses it is common for students to undergo some form of court room simulation. In the University of Portsmouth a high fidelity simulated (mock) court room was opened in February 2010 by the Portsmouth Business School. The mock court room (Fig. 2) is used by a number of Faculties, and provides a suitably intense experience of court room processes to students. The court room is really a room with unusual furniture laid out in a particular way, with the illusion enhanced by a few special effects, such as a coat of arms, and a witness box. Never the less the illusion is quite strong, and is enhanced by the formal behaviour of the role playing participants (judge, council, ushers etc.). Equipped with closed circuit television, it is possible to record and review each student's performance.

Figure 2: Mock Court Room (high fidelity court room simulation)

Court room simulations are usually used with students individually, as part of the assessment process, where students are cross examined about their report on evidence of their findings from a simulated investigation. Students often find the

experience very intense and even frightening. Part of this is due to the unusual experience of seeing their tutors dressed formally and behaving in an unusual role. Students are also encouraged to visit the public gallery of the local Crown Court. This gives another perspective on court processes and formality, but can be somewhat hit and miss, as it depends on the cases being heard, and which part of a trial that is seen (for example hearing evidence is often a fairly brief part of many trials, and expert witnesses are uncommon).

Using Second Life as a simulation environment

Second Life seizure simulation

The Second Life seizure simulation is based on student prototypes developed on an undergraduate human computer interaction unit (HUCID). The simulation consists of a location in which a target computer is placed, and a number of actions can be completed. Learning materials are usually located in the same area. The use of student prototypes meant that a number of different locations and styles of delivery can be built (Fig 3).

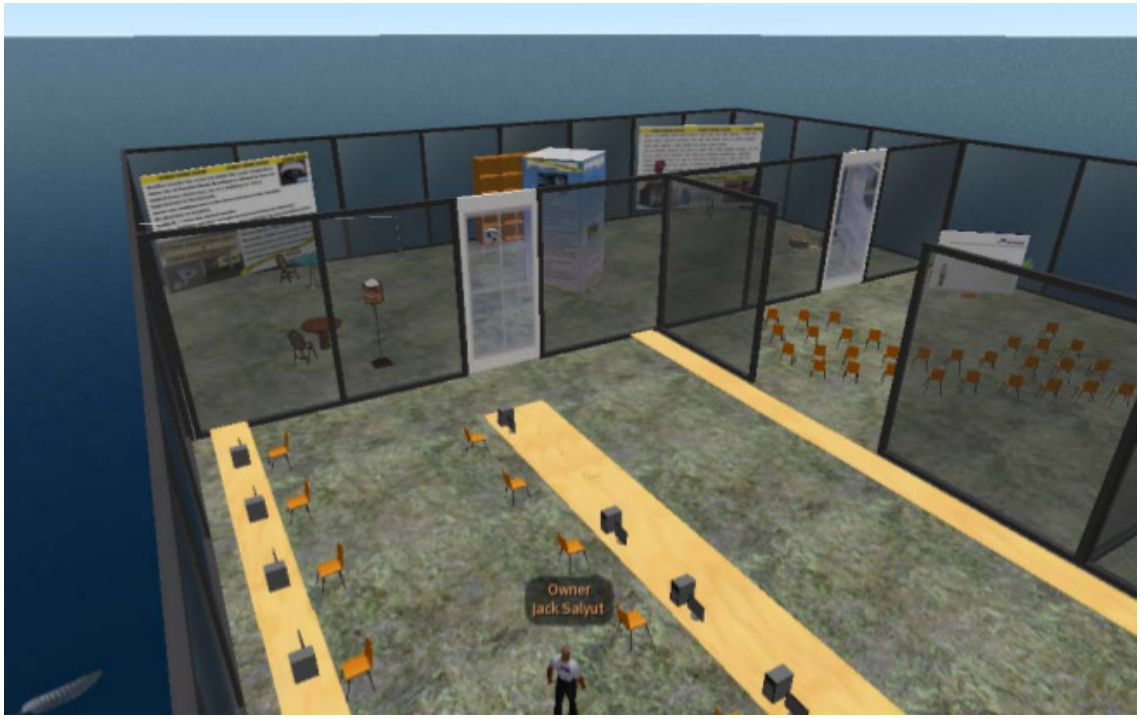

Figure 3: An example of a virtual seizure simulation environment in Second Life.

Extensions to the prototype involve more complex simulation of the seized computer's behaviour. An incomplete project involves the use of virtual network computing (VNC) remote control of a virtual pc running elsewhere (using the built in VNC server on the virtual machine software QUEM, http://wiki.qemu.org), and projecting its screen and behaviour into the virtual world. In this way the behaviour of a wide range of computers could be seen in Second Life.

A second extension will allow the Second Life target computer to be disconnected, opened and to have items removed, for example hard drives for later imaging. If

combined with a virtual computer, it would actually be possible to image the virtual pc, and provide the resulting image via a server.

The current Second Life seizure simulation can be accessed at any time by students individually, and is a useful adjunct to running a high fidelity simulation as a class exercise. 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 can use it at any time with the presence of a tutor being optional (Crellin & Karatzouni, 2009).

Court room simulation

The Second Life court room simulation included a building with all the main components of a court house (including not only the court itself but witness waiting areas, jury consideration areas etc.). Fig. 4 shows the court room, with the main features, the bench, jury box, and witness box.

Figure 4: Court Room Simulation in Second Life

The court room includes a number of animated avatars which simulate some aspects of court procedure, for example a judge, simulated jury members and the accused. Other simulated roles have simple behaviours attached to them, for example an usher who can take a witness into the court room from the waiting area, an 'oathing tool' which allows a witness to swear in, and lawyers who can ask a series of simple general questions. Automated note taking is enabled, so that a transcript of the court case can be reviewed at a later date, or submitted to tutors for feedback. In addition, learning materials on the nature and processes involved in a court are available within the simulation. These use Second Life techniques such as note cards, and media slide shows to introduce the features of a court in an on-demand mode.

A number of extensions to the court room simulation are proposed including the introduction of an automated guided tour of the court room and related rooms, and more sophisticated scripts for the court room 'role' avatars. This will assist with the difficulties caused by the court room being quite cluttered with objects, which can make navigation through the spaces difficult, particularly for novice users.

Student feedback and response

Unit feedback from two cohorts of the digital forensics unit have been collected (Table 1). The teaching content of the two years (Year01 and Year 02) was similar with no major changes between the two years. The digital forensics unit was one of the more popular units studied in the first academic year, but was much less popular in the second year. In both years the amount of face to face simulation was constant (slightly increasing in the second year). In the second year more exposure was given to the Second Life simulation.

The two cohorts were however markedly different. The first cohort included several students with law enforcement experience, and systems administration experience, whilst most of the students in the second cohort came from other courses, or from less relevant working experience. Students in the first cohort were much more likely to spend additional time on self directed work (as evidenced by out of class lab attendance). Qualitative comments from the two cohorts were also quite different. In year01 the comments about the simulation exercises were almost ecstatic, in year02 very few students commented on the simulation exercises, but often commented on the difficulty of the material.

Table 1: Unit feedback averages for the Digital Forensics Units

Year of Delivery	Content	Interesting	Delivery	Enjoyed
Year01	4.33	4.89	4.22	4.78
Year02	4.25	4.13	3.75	4.13

The data does not allow any definitive conclusions, however some patterns do seem to be indicated. Although simulation may be seen as a way of increasing engagement with students, the effect is likely to be more complicated. Students with higher levels of engagement with the subject matter seem to find using virtual worlds for the simulations enhances the activity. Those with less subject matter engagement seem to find that simulation simply increases the apparent complexity of the material, rather than illuminating and enhancing.

Teacher feedback and response

One of the problems with conventional simulation is that it usually requires a great deal of setting up for each run of the simulation. This makes it difficult to run a simulation for each individual student. For example it usually takes at least three hours of staff time to set up when a court room simulation is run with individual students giving evidence as part of their assessment. Second Life based simulations can however be 'left in place' or packaged, so that they are always available. Running the face to face court room simulation (with about 15 minutes of cross examination for each student) then takes approximately five to eight hours of

staff time, and involves four members of staff. A Second Life simulation can be run by a student on their own, using the automated role playing avatars. A student is able then to repeat the exercise as many times as they wish, and can also record the session for future reference, or for formative feedback.

Some aspects of the tasks involved in digital forensics have proved very difficult to simulate effectively in Second Life. For example a real cross examination does not involve a fixed sequence of questions, but rather involves a dialogue between the lawyers and witness, as the lawyers attempt to extract the real meaning and significance of the evidence.

Conclusion

Simulation can operate at different levels of fidelity. High fidelity simulation tends to involve more work each time the simulation is run than a lower fidelity digital simulation. The extent that simulations at various levels of fidelity increase engagement is complex. Different groups of students respond to the simulation exercises in different ways, in part based on their motivation for undertaking the course and on their previous work experience. Ease of use of the simulation (for both teacher and learner) seems important. Second Life has the advantage that it is relatively easy to use with little initial preparation, almost at a whim. However it can be frustrating for novice users who experience difficulty moving around in buildings, between furniture and comprehending the interface.

Future development and enrichment of the Second Life simulations will enable both further evaluation of the relationship between individual students engagement with the subject and the different forms of simulation.

Acknowledgements

Students on the Human Computer Interaction Design unit at the University of Portsmouth who provided earlier versions of the simulations discussed in this paper. Students on the Digital Forensic Investigation unit at the University of Portsmouth, who provided feedback on various aspects of the units delivery and teaching. Aline Riss, an exchange student, from the Université de Technologie de Belfort-Montbéliard, France, who developed the court room simulation in Second Life, and exchange student Anita Panayotova, from the Technical University of Sofia, Bulgaria who developed parts of a seizure simulation.

References

Andrianoff, S. and Levine, D. (2002) Role Playing in an Object-oriented World. *ACM SIGCSE Bulletin - Inroads: paving the way towards excellence in computing education*, **34**, 1, 121-125 doi: 10.1145/563517.563386

Association of Chief Police Officers of England (ACPO) (2007) Good Practice Guide for Computer Based Evidence. Retrieved 21-May-2010 from: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

Crellin, J., Chandler, J., Duke-Williams, E. and Collinson, T. (2009) Virtual Worlds in Computing Education, *Computer Science Education*, **19**, 4, 315–334.

Crellin, J. and Karatzouni, S. (2009) Simulation in Digital Forensic Education, Proceedings of 3rd International Conference on Cybercrime Forensic Education and Training (CFET3) (BCS SG) Conference. Retrieved 21-August-2011 from: http://eprints.port.ac.uk/1598/
L-3 Communications (2009) Link Simulation & Training: Setting the Standard for 80 Years. Retrieved 19th August 2011 from http://www.link.com/history.html

Losavio, M., Keeling, D.W., Elmaghraby, A., Higgins, G. and Shutt, J. (2008) Implications of Attorney Experiences with Digital Forensics and Electronic Evidence in the United States, *Systematic Approaches to Digital Forensic Engineering, 2008. SADFE '08. Third International Workshop*, pp.79-90.

Zowghi, D. and Paryani, S. (2003) Teaching Requirements Engineering through Role Playing: Lessons Learnt, *RE '03 Proceedings of the 11th IEEE International Conference on Requirements Engineering* 233- 241, ISBN: 0769519806