Experiences Using the Forensic Case Generator in Undergraduate Programmes

Michael Jones
Department of Computing & Informatics
Bournemouth University
Poole BH12 5BB, UK
mwjones@bournemouth.ac.uk

***Abstract*- The Forensic Case Generator (FCG) [1] has been developed and used over the past 6 years at Bournemouth University. The objective is to support the learner progress towards becoming a reflective practitioner [2] by providing an environment where the learner gains relevant skills and understanding with minimal direct support. We have evaluated the use of the FCG in terms of learner achievement and motivation.**

I. Introduction

The FCG has been used with nine Level 5 cohorts of students, six in a module within a computing framework, and three in a module in a forensic science framework. A total of 317 students have each investigated two assessed cases, as well as a number of formative exercises. In addition the computing cohorts have engaged in assessed group investigations as part of a separate project management module.

II. The Forensic Case Generator

The FCG hides data using a range of encoding and embedding techniques. There are four phases of the FCG are: data generation, encoding and embedding, file system generation, and feedback generation. The main focus is on file forensics, main due to the time-frame involved (one semester) and the limited prior skills and understanding of the students. The majority of the software is written in Java, and uses a number of publicly available APIs. The global dataset used as the basis for all the case has been constructed from publicly available data sources.

III. Stretching Plausibility

A greater variety of hiding techniques are used within a single case than would be situation in a 'real-world' investigation. The use of many techniques of varying complexity facilitates a more graded learning experience. It also enables a degree of discovery – some of the techniques employed are not explained to the students in advance.

IV. Enhancing Plausibility

A digital investigation can be considered to be a special case of an all-knowledge data-mining problem, where the data has been hidden deliberately and is to be retrieved at a later date. Unless the investigator has access to the retrieval processes, he or she needs to use a combination of induction, deduction and abduction to retrieve the data. No two investigations are identical. The unique dataset and file system created for each student via the FCG replicates the essential elements of a 'real-world' investigation.

V. The Crimes

The FCG has an extensible set of 'crimes' that can be investigated. Examples include smuggling (drugs, cigarettes, arms), human trafficking, bank robbery, murder (serial), DDoS (command and control configuration only), car theft (to order), and planned terrorist attacks and campaigns.

VI. Developments – Hiding Techniques

The extensible nature of the FCG facilitates the inclusion of additional hiding and encoding techniques. Some IT-related techniques have been added, although the majority of the techniques added can be characterized as requiring 'lateral thinking' of the learners. Examples include the use of Braille and acrostics.

VII. Developments – Cases

Learners have consistently exceeded expectations in terms of their ingenuity, with the result that cases have become more sophisticated. In a recent assessment, learners were presented with multiple files, all symmetrically encrypted. Learners had to construct and then use a dictionary to unlock one file, which contained hidden passwords, some of which unlocked the other files. These other files contained the details of a planned terror attack. This was a group assessment, and it was necessary to supply the first password to most of the groups. More emphasis will be placed on conducting a dictionary attack in the next presentation of the module.

VIII. Developments – Marking Scheme

Initially, considerable weighting was given to the retrieval of the data. This had two effects: the average mark was much higher than on other modules in the same level, and learners focused on retrieval at the expense of interpretation and presentation. In recent presentations the marking scheme has been modified, and this has had the desired effects.

IX. Developments – Marking

The reports are marked manually, using traditional means. The unique nature of the cases potentially presents a significant marking overhead. A marking component has been added that compares the spreadsheet submitted by the

learner(s) with the one created for that case by the feedback generator within the FCG. The marking component has been modified to allow some leniency (e.g., minor typing errors), although this can changed in the FCG configuration.

X. Retrieval Rates

The mean number of data items retrieved is generally between 90 and 95%, and this applies equally to the computing and forensic science students. This is to be expected, as the greater general IT knowledge of the computing students is compensated for by the greater exposure of the forensic students to forensic processes. The distribution of retrieval is positively skewed with a minimum generally around 80%.

XI. Measuring Student Response

As the learners are not in a position to compare their experience with one where (for instance) every student was supplied with the same case, the focus for evaluation has been on the evidence of learner achievement and motivation.

It is reasonable to assume that each learner has retrieved the vast majority of the hidden data himself or herself, even if he or she received assistance

A differential rubric has been used for the calculation of the overall mark in these coursework-only modules. The final mark is calculated based on 60% of the higher mark and 40% of the lower mark. A learner achieving a high mark on the first assessment need make little or no effort on the second (there is no pass mark for each assessment). Our experience has been that learner achievement and motivation has remained throughout the module, as the differential rubric has little effect.

The correlation between first and second assessments has been in the range 0.3 to 0.65. The higher figure led to a redesign of the assessments, to increase the differentiation.

XII. Weaker Students

The interpretation can be compromised if too many items are missing. This tends to create the possibility that weaker learners will be doubly punished, in terms of retrieval and interpretation. Two approaches have been taken to avoid this. In many of the assessments, the details of multiple crimes (robberies, thefts, murders) have been embedded. Where a single crime is involved, an intermediate (retrieval) milestone has been added. Once the retrieval spreadsheets have been submitted, the complete spreadsheet is supplied, enabling a level playing field for the interpretation.

XIII. Observations

A number of learners have professed (during the assessment) that they are highly motivated to find everything and will want to know which techniques have eluded them. But, so far, not one learner has requested this information once the assessment has been completed.

The second observation is that each cohort is as motivated as the last. Information regarding the modules will, not doubt, has been communicated between cohorts, but each reacts in more-or-less the same way. The one exception has been the most recent computing cohort. A few students did not engage with the second assessment at all. Personal circumstances were certainly a factor in some cases, but this will need to be monitored.

The third observation is that learners need very little support after the initial few weeks. More senior students augment the support team during these early weeks when few students have any experience of command-line tools. Once the first assessment is under way, very few students call upon tutors during or outside scheduled sessions. There is strong evidence of learners willing to explain techniques to their peers, although this has not been systematically analyzed.

There appears to be no gender bias in learner achievement. One framework (computing) is predominantly male, and the other mainly female. Completion rates, student achievement and motivation are broadly comparable, although (so far) only the computing framework has seen learners whose motivation has declined during the delivery of the module. Anecdotally, the minority gender in each framework tends to achieve less well, but the volume of data gathered so far is insufficient for more detailed analysis.

XIV. Conclusions

The original motivation behind the development of the FCG was to facilitate the creation of a ‘learning studio’ where the focus was on analysis, rather than synthesis. Learners with little relevant background should be able to gain skills and understanding of most of the key elements of a digital investigation. And all learners should be able to progress without creating a bimodal profile. In these terms the development of the FCG has proved successful, with a high level of learner achievement and motivation being demonstrated across cohorts on two different undergraduate frameworks.

As the emphasis is on analysis, one would expect the practitioners reflection to focus on organization and process. In most aspects the performance of learners improves between assessments, indicating some level of reflection regarding the processes. In terms of the quality of the analysis of the results, however, it is the case that learners could reflect more on the implications of their findings. This area is still work in progress.

References

[1] M. Jones. *A Digital Forensic Case Generator*. 4th International Conference on Cybercrime Forensics, Canterbury, UK, 2010.

[2] D.A. Schön. *Educating the reflective practitioner: Toward a new design for teaching and learning in the professions*. San Francisco, Jossey-Bass, 1987.