What Makes a Computer Forensics Project?

David Chadwick, Diane Gan, Dimitris Frangiskatos

C-SAFE Centre
University of Greenwich

It is a constant challenge to identify suitable projects for students who are studying computer forensics. An appropriate project must have a relevant theoretical element and an implementation. Projects are meant to be instructive and should engage the student. At the University of Greenwich, the final project for the MSc award is worth 60 credits out of a total of 180 credits for the entire masters award. The project therefore is a substantial piece of work (suggested 300 hours student time), is minimally supervised (students are expected to really work on their own with occasional guidance from the supervisor) and is expected to be non-trivial in nature (exploring a specific topic in depth rather than a wide topic in a shallow way). Lecturers post suggested projects on a web site, as a starting point but it is expected that students will take these ideas much further or even come up with their own ideas.

The C-SAFE team identified various issues that could arise with forensics based projects particularly at masters level. The team considered that a forensic topic should be in one of three main areas of investigation:-

1. Solving an actual forensic problem
2. Researching a new forensic methodology
3. Comparing forensic tools with each other on a range of relevant criteria.

The first option is, of course, the preferred option as this is precisely what the forensic investigator is expected to do in the real world. It encompasses the basic skills of investigation, demonstrates the student’s ability to carry out an investigation in a methodical manner abiding by all the rules of data-handling, chain of custody and legal etiquette etc. However this is perhaps the most difficult project to arrange. The problem here is where do unsolved cases arise that can be given to students? Or how do supervisors find the time to construct fictional cases that are to be sufficiently different from each other that students cannot collude?

The second option suggests dealing in leading-edge technologies and methods and, as such, might be beyond the ability of many students. It is perhaps more appropriate at PhD level but a good masters student may suggest an area they wish to tackle and providing the project is small enough and is well scoped then this is a possibility. The problem here is how can we, the supervisors, keep up with the latest ideas and be aware of what seem promising areas of research? Two examples of projects that fit this category are the “Design and development of a flash memory based application for the automated retrieval and presentation of digital forensic data on Windows platforms in a timed environment” and “A prototype forensic tool kit for investigating GPS devices with analytical capability to aid the investigator”.

The last option is perhaps the easiest option for the student. They would need to define and justify the criteria they choose for comparisons to be made. In addition they would need to actually trial the tools under testing conditions to really gain useful findings. The problem here is that projects such as this often descend into trivial list-making without any real understanding of the tools themselves and what investigators consider useful features.

Other factors to be taken into consideration are

- Projects need to prepare graduates for a career in forensics
- Computer crime is on the increase
- Practitioners need to be aware of underlying forensic theory as well as practice
- Computer forensics is multi-disciplinary
- Projects need to be fun and challenging and capture the imagination

It is important that students find a project that they are passionate about and this will naturally be reflected in the quality of the final product delivered. At the University of Greenwich we have been fortunate to have a number of excellent projects submitted which will be presented as a case study.