

# Computer Forensics Workshop for Undergraduate Students

Derek Bem and Ewa Huebner

School of Computing and Mathematics

University of Western Sydney

Penrith Campus, Locked bag 1797, Penrith South DC NSW 1797, Australia

{d.bem, e.huebner}@scm.uws.edu.au

## Abstract

This paper describes our experience in the design and implementation of a computer forensics specialisation for the Bachelor of Computer Science degree and its capstone subject Computer Forensics Workshop. Our motivation for introducing this specialisation was to respond to the growing demand for professional services in computer forensics by the government and industry as well as to attract undergraduate students back to computing. Computer forensics is an emerging multidisciplinary field with foundations in computer science and law, and academically it is best positioned as a stream in general computer science degrees. The capstone subject in the specialisation, Computer Forensics Workshop, is practically oriented with a substantial laboratory component. The subject is taught by a team of academics, each contributing their expert knowledge in operating systems, file systems, network security and cryptography. The aim is to prepare the students to enter the job market as a professional computer forensics specialist, either in a law enforcement agency or a business organisation relying on computer information systems.

*Keywords:* Computer Forensics education, curriculum design

## 1 Introduction

The computer forensics specialisation for the Bachelor of Computer Science degree at the University of Western Sydney ("UWS Handbook," 2007) was designed in 2005, and first offered in 2006. Our motivation was twofold. Firstly we could see the rapidly increasing demand for computer forensics professionals, and secondly we wanted to reignite the interest of prospective students in computer science as it was in noticeable decline after the Y2K bug and the dot-com crash.

Computer forensics is a multidisciplinary field founded primarily on computer science and law. We previously had a solid program in computer science with a

specialisation in systems programming, so the groundwork on which to build a computer forensics stream was already there. Topics like operating systems internals, file systems, computer organisation, data representation, information security, computer networks and the operation of a computer system were adequately covered in existing subjects. To create the forensics stream we included a law subject to ensure that students are aware of the legal environment, especially the rules for handling evidence. Another new subject was the Computer Forensics Workshop, which was designed from scratch to serve as a capstone for the computer forensics stream.

To ensure that students obtained the maximum benefit from attending the workshop, we set prerequisite subjects, namely Operating Systems, Systems Administration Programming and Network Security. To obtain the specialisation in computer forensics students also have to complete the following subjects: Computer Networks and Internets, Computer Security, and Information Security. This complements a generic computer science program, which covers all core topics recommended by the ACM/IEEE-CS Computer Science Curricula (ACM/IEEE-CS, 2001).

Computer Forensics Workshop ("UWS Handbook - units," 2007) is the defining subject in the stream. It is delivered as a combination of weekly lectures and laboratory sessions. The hands-on component is obviously very important in a workshop based subject, so the laboratory sessions last for 4 hours, twice the time compared with other subjects. The assessment is mostly based on laboratory reports, which students complete in their own time. There are also two assignments, again completed outside scheduled hours. Because of the practical nature of the material covered, we decided that a final written exam would not be a suitable assessment tool.

## 2 Design and Structure

The computer forensics capstone subject consists of weekly lectures and a series of investigative workshops that put into practice, in a computer forensics context, many of the technical concepts and skills covered in earlier pre-requisite units. Despite the very practical nature of the subject we decided to retain the lecture component. The role of lectures in the Computer Forensics Workshop is not only to introduce specific forensic topics, but also to provide computer forensics context to the knowledge the students already have.

Let us consider the topic of file systems. The subjects like Operating Systems and Systems Administration Programming cover the underlying principles and specific common implementations, like Linux Ext2 and Windows NTFS. Forensically this is not sufficient, because students also need to understand data hiding techniques (Huebner, Bem, & Wee, Spring 2006), recovery of deleted files, and similar topics. Another good example is the analysis of time stamps in the log files and the file system which allow for the reconstruction of the events leading to or constituting a criminal act. Not only are the clocks in various networked systems not perfectly synchronised, various operating systems treat time stamps in file systems in subtly different ways. The lectures provide a foundation for the workshop sessions by exposing these issues, and they also rely heavily on the computer science knowledge the students already have.

Another issue we faced in designing the curriculum was the wide range of topics in computer science we had to cover. It became obvious early on that no one lecturer has both sufficient breadth and depth of knowledge to be able to handle all components of the subject. We decided that the best approach is to use a team of academics. In our case there were five lecturers covering in-depth knowledge of operating system, files systems, computer security, network security, systems programming and administration as well as computer organisation and architecture.

Several academics in this group are also actively involved in research in computer forensics (Bem, 2007). This ensures that as this field develops we will maintain the state of the art content in the subject, and also provide a path for students wishing to undertake research projects at Honours, Masters and PhD level.

### **3 Content and Outcomes**

Unlike other fields in computer science, no guidelines or recommendations exist for computer forensics curricula, so we had to rely mostly on our own research and professional experience in the related fields. The same process was followed by other universities introducing computer forensics into their curricula at the time (Gottschalk, Liu, Dathan, Fitzgerald, & Stein, 2005; Hentea, Dhillon, & Dhillon, 2006; Yasinsac, Erbacher, Marks, Pollitt, & Sommer, 2003). The characteristic feature of our approach was to focus on first principles instead of relying on specific forensic software tools. This was possible because of the strong computer systems background of our students, who complete subjects covering systems programming, operating systems and system administration programming before studying computer forensics topics.

The first topic we covered was media preparation and copying techniques, so that students understand the issues involved in the preparation of forensically clean storage media to accept image copies of suspect media as well as performing an image copy from multiple storage media types without altering the source media. This topic is very well suited for laboratory exercises, and allows for the application of manual techniques using the disk imaging

dd utility and industry forensic software suites. "dd" most likely stands for "data definition", but the origins of this acronym are not certain; it is a program whose purpose is the low-level copying and conversion of data ("The Open Group Base Specifications Issue 6," 2004). There is also scope for practicing the maintenance of the chain of custody as well as the required standard of documentation and reporting procedures.

The next topic was file system structures and file type identification techniques, analysis of time stamps as well as searching for and identifying hidden data. We chose to cover in detail the prevailing file system formats in Windows and Unix derivative systems, namely FAT, VFAT, NTFS, Ext2 and Ext3. With general knowledge of file systems gained in prerequisite subjects students were well prepared to handle the necessary details. The laboratory work was used to reinforce the techniques used to locate and identify data and files that are hidden on the media, and to reconstruct, in part or totally, deleted data or files that remain on the media. Again we used both simple manual tools like hex editors and dedicated forensic tools like Sleuthkit (Carrier, 2007). In order to make it possible for students to complete the work in the available time when using hex editors, we used floppy disk images. The analysis of an average size hard disk image with a hex editor is simply too time consuming, although in a laboratory environment the student can be given hints which limit the scope of the search. It should also be remembered that most if not all existing industry forensic software tools are developed from hex editors (Fleischmann, 2007), so it is important that students understand the nature of simple tools and their inherent limitations.

As a prerequisite to the Computer Forensics Workshop students complete three security related subjects: Computer Security, Information Security and Network Security. These subjects cover security issues exhaustively, so there was no need for a substantial security component. It was still important to impress on students the consequences of applying computer security measures, including cryptography and steganography, in a forensic setting. We also introduced new computer forensics techniques like live system investigations and memory forensics. The former was also used to demonstrate how much information can be gained from the system without privileged access, and the latter to show that clear text including passwords can be extracted from a memory image. It is also important to appreciate that in the real world a computer forensic investigation is usually part of a larger case, and often conventional investigative techniques can deliver passwords, keys and other means of gaining access to a protected system.

Another important set of skills for a computer forensics investigator is the ability to extract data from log files maintained by the operating system, web and email servers, network proxies and firewalls as well as caches maintained by both server and client machines. These topics were covered in several modules with general and network related system logs covered separately, and included the analysis and interpretation of extracted log and cache data. In laboratory tasks students were exposed

to both Unix-style and Windows-style logs. Because of the different philosophies behind these systems it was important for us to include both in this and other topics. Documentation and presentation of the results obtained from the above activities was also part of the laboratory work. This allowed us to expose critical issues related to clock synchronisation, and the impact they have on the forensic reconstruction of system events.

The final topic was how to prepare a system and network to best support subsequent intrusion and activity detection. We wanted to make sure that students realise the importance of a forensic plan for any computer installation, and are able to formulate such a plan in various environments. This is different from securing and protecting the system, and deals with processes and procedures to handle events after the fact.

It is very difficult to recommend a single textbook for a computer forensics subject, and standard computer security textbooks give very little, if any, coverage to computer forensics related topics (Pritchard & MacDonald, 2004). We covered many topics, and each lecturer was able to specify what they considered to be the best resources for the area covered. Also the course was based heavily on detailed lecture notes and electronic materials in printable format, which allowed each student to collect and print their own set of materials. In the end we recommended to students a good general textbook (Jones, Bejtlich, & Curtis, 2005).

#### **4 Laboratory Experience**

The laboratory experience plays the central role in a workshop style subject. Students have to be able to test the knowledge they gained by performing practical tasks, which in the professional setting would be part of a computer forensics investigation. However, there are some issues in an educational environment which need to be resolved as reported in Gottschalk et al., 2005. Firstly, some of the investigative procedures require fully privileged access to the computer system. The best solution is to build a stand-alone dedicated laboratory with limited controlled access to the network to create a safe 'sandbox' environment. This was not possible in our case, as all laboratories serve many different purposes, and it would not be economically viable to limit the usage to one subject only. We solved this problem by using Helix, a customised distribution of the Knoppix Live Linux CD (E-fense, 2007), which boots from a CD ROM and uses memory-mapped disks. The content of the hard disk is never changed, and it is easy to restore the normal environment for the next class by rebooting all systems. We also designed the laboratory work in such a way that in most cases privileged access to the system was not required.

Another issue we considered was whether it is necessary to give students access to commercial computer forensics software packages. It seems obvious that being able to work with a commercial package would enhance the general student experience. The real question is whether it is strictly necessary in order to give students a well rounded education. After reviewing the market we

decided that it is not so. We believe that it is of greater benefit to a student to be able to work from 'first principles', and to be able to conduct the investigation using simple tools like hex editors and command line utilities. Some exposure to dedicated software tools is also desirable but only after students learn to operate at the lower level of abstraction.

The computer forensic software companies are mostly small organisations, and typically they are not willing to grant free educational licences. One notable exception is ProDiscover ("Computer Forensic Tool for Law Enforcement," 2006), which offers a cut-down version of their software free of charge. This version was not available at the time of the first delivery, and we intend to include it this year. Another popular commercial package is the Forensic Toolkit (FTK) from AccessData. This software can be installed and used on any machine in evaluation mode, which restricts the number of files which can be analysed. The current limit is 5000 files, which makes it unsuitable for commercial work, but does not affect the educational application, as the test cases studied are limited in size. We demonstrated FTK to students in a lecture, and we intend to use it more extensively for laboratory work in this year's delivery of the Computer Forensics Workshop.

There are also various freeware products, for example Sleuthkit and Autopsy (Carrier, 2007), which are packaged in the Helix distribution. This is sufficient to demonstrate to students how such tools work, even though they do not get specific training or certification to use any particular product. We do not see this as a problem. We believe that students can get sufficient exposure to expensive commercial tools by using restricted versions of software offered for evaluation.

All commercial distributors offer specific training courses for their products, and it is the usual practice for employers to finance such courses for their professional employees. The market changes continuously and it is not the goal of university education to give students specific skills with specific software products. Rather the students should be given sufficient foundation knowledge and learning skills to be able to gain the full benefit from commercial training if and when it is appropriate.

#### **5 Career Paths**

The perennial issue in academia is to what extent the undergraduate education should prepare the students to be immediately successful in the job market. This is particularly so for narrow specialisations like computer forensics. Students select the degrees based on many criteria, but a young person has to see the course as attractive and exciting in the first place. There is an important moral issue here; is it fair to encourage students to select a specialisation when it is not certain that they will be able to find a corresponding job?

This is a difficult question to answer. Universities cannot just prepare the students for existing jobs, they have to look further into the future to see what jobs will be available in three, five and ten years' time. This is what serves the students and the industry best, even though at

the time it may not appear to be the right approach. Another issue is that there are established professions which can only provide employment to a limited number of people, and educating more is counterproductive.

Let us consider computer forensics in this light. It may superficially appear that it is one of those self-limiting professions. After all, police and other law related organisations can only provide employment to a certain number of professionals. Fortunately computer forensics specialists can also find employment beyond this limited scope.

Most organisations base their very existence on the proper functioning of their computer systems. All of these are potential employers of a computer forensics specialist. The Australian statistics say (AusCERT, 2006) that most of the computer related crimes are not reported to any external agency, mostly for fear of negative publicity. This is likely to remain so in the future, and it means that the organisations will have to build an in-house capability to handle these matters. A computer forensic specialist is needed to devise the policy and procedures to be followed when and if a computer related crime is suspected or uncovered. Further a specialist should be able to handle the computer crime cases, to repair the damage if any occurred, and to assist the computer security specialist in setting prevention measures. In a small organisation the system administrator, the security specialist and the computer forensics specialist may all be the same person, but depending on the size of the organisation and its dependence on computer systems, each role may have a team of specialists assigned to it. Students completing the Computer Forensics specialisation in the Bachelor of Computer Science degree are well suited to these roles, either as a member of a specialised team or a general system support.

## 6 Feedback from Students

The prospective students were palpably excited by the Computer Forensics Workshop when it was first offered. Throughout the semester we repeatedly saw evidence of high levels of commitment and self-motivation. In the standard questionnaires answered by all University of Western Sydney students for each subject at the end of the semester our students expressed high levels of satisfaction with most aspects of the delivery and outcomes achieved in the Computer Forensics Workshop. There were 16 students in the 2006 delivery, and 14 of them completed the questionnaires. The Student Feedback on Unit questionnaire asks eight questions with ratings in the range from 0 to 5. We achieved a rating of above 4 in seven questions. The best four ratings were:

- The unit covered what the unit outline said it would: 4.7
- I was able to see the relevance of this unit to my course: 4.5
- The learning activities in this unit have helped my learning: 4.7
- The unit provided a reasonable amount of flexibility for study: 4.7

The weakest rating (3.8) dealt with clarity of guidelines in assessment. The second questionnaire, Student Feedback on Teaching, asks ten sets of questions regarding the quality of teaching, and one set of questions on difficulty of material and workload, with ratings in the range from 0 to 9. In all quality related questions we rated from 7.14 to 8.43, well above the University of Western Sydney average. The best rating (8.43) related to the question on coverage of current developments in the field, in the set dealing with learning and academic value. The weakest rating (7.14) again related to the assessment, specifically the value of feedback received by students.

The students also made a number of specific open-ended comments in relation to the best aspects of the subject, for example:

- The theory presented in the lectures related to and could be applied in a real world environment.
- Practical work was relevant to real world situations.
- I liked the wide range of content, and the many different views from different lecturers.

Both questionnaires show that in the opinion of students the weakest points of the subject and its delivery were related to the assessment of the work and the feedback received in the subject. This is the area which was probably affected by the team teaching arrangement, and the fact that students did not meet the same lecturer week by week. In future deliveries we will strive to alleviate this problem. One option is to provide some time at the beginning of each lecture for discussion of the previous week's work. This would naturally require more effort from each of the participating academics, but it would also give an opportunity to properly conclude each of the modules.

## 7 Conclusion

In our opinion the computer forensics stream we designed and implemented thoroughly prepares students to begin their professional career in computer forensics, starting as assistants for experienced investigators and developing into fully-fledged computer forensics professionals serving both industry and law enforcement agencies. The Computer Forensics Workshop itself can also be of value to practising computing professionals who wish to enter the field of computer forensics. For this reason we opened this subject up to so called non-award enrolments, which allow any member of the public to attend. Naturally this was vetted by the coordinator of the workshop to ensure that the prospective students had sufficient professional background to benefit from the study.

The body of knowledge in computer forensics, similarly to computer science – the discipline it emerged from – grows at a very rapid pace. It means that the specific content of the workshop will have to be constantly reviewed and adjusted. Our growing research strength in computer forensics also contributes to this process. We envisage that in future deliveries we will have to dedicate more space to memory forensics, live systems investigations as well as storage and systems virtualisation.

Another area which we would like to expand is the law content of the computer forensics stream. In particular it would be beneficial to the students who are likely to serve as expert witnesses to have practice in presenting evidence in a court of law. This kind of practice is useful to students in all forensic disciplines; it is not specific to computer forensics.

To summarise, the first delivery of the Computer Forensics Workshop was a demonstrable success. It is clear that it fulfilled students' expectations, and provided them with skills and knowledge that they will be able to apply in their professional life.

## 8 References

- ACM/IEEE-CS. (2001). Computing Curricula 2001 Computer Science. Retrieved 3 June 2007, from [http://www.computer.org/portal/cms\\_docs\\_ieeecs/ieeecs/education/cc2001/cc2001.pdf](http://www.computer.org/portal/cms_docs_ieeecs/ieeecs/education/cc2001/cc2001.pdf)
- AusCERT. (2006). *2006 Australian Computer Crime and Security Survey*: AusCERT.
- Bem, D. (2007). Computer Forensics. Retrieved 16 July 2007, from <http://www.cit.uws.edu.au/compsci/computerforensics/Technical%20Reports/index.php>
- Carrier, B. (2007). The Sleuth Kit. Retrieved 10 July 2007, from <http://www.sleuthkit.org/sleuthkit/desc.php>
- Computer Forensic Tool for Law Enforcement. (2006). Retrieved 20 December 2006, from <http://www.techpathways.com/ProDiscoverDFT.htm>
- E-fense. (2007). The HELIX Live CD Page. Retrieved 9 March 2007, from <http://www.e-fense.com/helix/>
- Fleischmann, S. (2007). WinHex/X-Ways Forensics [Electronic Version]. Retrieved 10 March 2007 from <http://www.x-ways.net/forensics/>
- Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S., & Stein, M. (2005). *Computer forensics programs in higher education: a preliminary study*. SIGCSE Technical Symposium on Computer Science Education.
- Hentea, M., Dhillon, H. S., & Dhillon, M. (2006). Towards Changes in Information Security Education. *Journal of Information Technology Education, 5*.
- Huebner, E., Bem, D., & Wee, C. K. (Spring 2006). Data hiding in the NTFS file system. *Digital Investigation, Volume 3*(4).
- Jones, K., Bejtlich, R., & Curtis, R. (2005). *Real Digital Forensics: Computer Security and Incident Response*: Penguin Books Pearson Publishing.
- The Open Group Base Specifications. (2004). Issue 6. Retrieved 21 March 2007, from <http://www.opengroup.org/onlinepubs/009695399/utilities/dd.html>
- Pritchard, J. J., & MacDonald, L. E. (2004). Cyber terrorism: A Study of the Extent of Coverage in Computer Security Textbooks. *Journal of Information Technology Education, 3*, 279-289.
- UWS Handbook. (2007). Retrieved 10 July 2007, from <http://handbook.uws.edu.au/hbook/course.asp?course=3506.3>
- UWS Handbook - units. (2007). Retrieved 10 July 2007, from <http://handbook.uws.edu.au/hbook/unit.asp?unit=300447.1>
- Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., & Sommer, P. M. (2003). Computer Forensics Education. *IEEE Security and Privacy, 1*(4).

