TEACHING 'LINUX AS A FORENSIC TOOL' (ONLINE) TO EUROPEAN LAW ENFORCEMENT

Paul Stephens
Forensic Computing
Department of Computing (Academic)
Canterbury Christ Church University
UK

Abstract

The purpose of this work is to discuss the implications of creating, delivering and maintaining an online MSc level course in forensic computing. There are unique issues associated with this endeavour as the development group for this particular module is comprised of experts from law enforcement and academia from across the European Union and the students are serving police officers from the member states. This paper discusses the reasons for running the course online, the issues associated with this change, and the challenges faced by the development team.

Introduction

In 2002 under the European Commission (EC) funded Falcone Programme (European Commission, 2002), an expert group comprising law enforcement officials and academics from across the European Union held several meetings to identify areas for improvement in training for high tech crime investigators. Having examined the training programmes available in a number of member states, the group concluded that a European approach to cybercrime training and education was required. The panel of experts recommended that university accredited training in computer forensics be provided to law enforcement officers that is consistent throughout the member states. Furthermore, they agreed that provision should be made for sharing of training materials and the development of new resources in an attempt to minimise workload and promote best practice (Ó Ciárdhuain et al., 2003).

The following year several members of the Falcone Programme expert group began to carry out these recommendations. The funding was made available through the AGIS Programme (European Commission, 2006) under the title Cybercrime Investigation — Developing an International Training Programme for the Future. Microsoft and several of the organisations involved in the development provided additional funding. The projects ran between 2001 and 2008 and as of January 2008, there were seven courses that had been developed for use by law enforcement organisations internationally:

- Introductory IT Forensics and Network Investigations (2003–2004);
- Applied NTFS Forensics (2005–2006);
- Intermediate Internet Investigations (2005–2006);
- Intermediate Network Investigations (2005–2006);
- Linux as a Forensic Tool (2006–2008);
- Mobile Phone Forensics (2006–2008);
- Wireless LANs and VOIP (2006–2008).

Whilst the early stages of the projects concentrated on the Windows-based forensics, the latter stages show how the field is fast developing, requiring an understanding of different operating systems, a wider range of techniques, and a need for frequent updates to all courses.

Under ISEC (European Commission, 2008) the latest incarnation of this project group (which now includes representatives of Europol, Interpol, and the UN ODC) suggests that three new courses be developed:

- Advanced Scripting
- Malware Investigations
- Live Data Forensics

In addition to these new courses it is suggested that all courses developed so far be updated (sponsored by Microsoft) and that all courses be run as an MSc scheme to be accredited by University College Dublin, Ireland in the first instance.

This paper focuses on the development and upgrade of the Linux as a Forensic Tool module.

Development of the Linux as a Forensic Tool Course

The Linux as a Forensic Tool course was developed for a number of reasons. One that is particularly important is that Linux is free and open source making it extremely attractive to publicly funded services such as the police, who investigate the crimes, and educational establishments, who teach the theories and principles of digital investigation. Many of the organisations now involved with the ISEC project also have a wider remit than just the EU, e.g., Interpol and UN ODC, are making these courses available to poorer nations such as those found in Africa and the Indian sub-continent, many of which cannot afford expensive hardware and software.

Open source software can be easily modified and added to. Linux is also better suited to many forensic tasks as opposed to Windows. For example, you can mount disks read only and disallow executables from running. As well as these

advantages, Carrier (2003) argues that as these tools can dramatically affect people's lives by demonstrating innocence or guilt, they should be subject to a more stringent process of review than is available if the code of such systems is not published. Instead, he promotes an open-source approach whereby the processes and procedures used are clearly defined and subjected to systematic review and debate.

Some users of Linux argue that making the tools easier to use is one way of improving the numbers involved in carrying out digital investigations. Others however, claim that an investigator should be equipped with a more advanced knowledge of computing and therefore advocate the introduction of programming skills. The proposed ISEC Advanced Scripting course aims to provide such training.

The Linux as a Forensic Tool course was piloted in April 2007 at The Garda College, Templemore, Co. Tipperary, Ireland as a one-week course. Following evaluations by the students, trainers, training designer, and quality assurance experts it was decided that the course be split into a two week course due to its complexity. The first week would cover the basics of Linux in a forensic computing context and in the future will be run as an online module. Week two will cover the more in depth forensic features of Linux and the associated tools. Issues that arise concerning the updating of this course include changes:

1. in the Linux operating system installation and setup procedures, i.e., updates of operating system and user interface;

2. involving the update of the forensic image's operating system and file system, i.e., the update from Windows XP to Windows Vista and the introduction of features such as BitLocker drive encryption;

3. the introduction of and updating of free and open source tools, i.e., installation and use instructions will differ as well as better tools becoming available and others becoming obsolete;

4. the updating of forensic tools associated with forensic image production, i.e., potentially the EWF format could change with a new version of Encase;

5. the updating of anti-forensics techniques, i.e., new methods of obfuscating will need to be introduced into course material to make students aware of such approaches;

6. better hardware than is currently specified will be required, i.e., one aspect of the course involves running a suspect Windows image in a virtual machine on a Linux machine — Vista requires better hardware than XP; and

7. concerned with updating a class-based course to an online module, i.e., course material will need to be in a format suitable for self-paced, distance learning and suitable support structures will need to be in place.

Problems 1–6 above pose no major challenges, as part of the original course development and training team are working on these issues at present. The current course focuses on several forensic tools that have been well tested in the field, particularly by the Belgian Federal Computer Crime Unit. Some evaluation of these tools has also taken place in the laboratory by NIST (2008) and by Childs and Stephens (2008). Many of these tools are command line based and require an in depth knowledge of the Linux operating system as well as a good understanding of file systems. This can cause investigators major problems and may be one of the reasons why there is not a larger uptake of such tools. Even when there is a GUI front-end, such as that provided by Autopsy it is in need of improvement. Some of the work currently underway is intended to make these Linux tools easier to use, especially for those investigators coming from a Windows point-and-click environment (see for example Bennett & Stephens, 2008). Almost all of these tools are free and open source and therefore those with a programming background can enhance these tools. Although some law enforcement agencies are doing this, such as the Dutch National Police Agency, many do not have the expertise or the resources. This may therefore fall to the open source community with help from academic institutions. Issue number 7 above: converting a class-based course to an online module, will now be examined in more detail.

Reasons for Online Development

One of the major reasons for week one of the Linux as a Forensic Tool course being run online is concerned with cost issues. Funding estimates and project managers had originally only planned for a one-week course, however following the evaluations the two-week course was deemed necessary. The evaluators also concluded that there needed to be a sufficient break between week one and week two for students to experiment and for knowledge to ‘sink in’, thus escalating costs further. Although at present only week one of the Linux as a Forensic Tool course is being converted to an online module, this development is being seen as a pilot for all courses that will form part of the MSc scheme. Part of the reason for this is the cost savings such a measure would bring. Another part of the reason is

to make the training available to the widest possible audience with the fewest possible instructors. This is important, as even in the UK there are not enough trained professionals to deal with the enormous amount of digital evidence. A report by UK MPs stated, "We have around 140,000 police officers in the UK. Barely 1,000 of them have been trained to handle digital evidence at the basic level and fewer than 250 are currently with Computer Crime Units or have higher level forensic skills" (Eurim, 2004). Whilst this situation may have improved in the past five years, anecdotally there is still a lack of trained computer forensics investigators. Finding instructors for the course is also difficult. Indeed the current upgrade was meant to occur during February 2009 but has had to be postponed until October 2009 due to a number of trainers being unavailable.

Issues Unique to this Course Development

There are several issues unique to the development of the Linux as a Forensic Tool course. Firstly, the course development team is truly international. Currently there are five trainers (including the author) from five separate countries: The UK, The Netherlands, Norway, Finland and Germany. In addition, the managers and other course developers such as the quality assurance experts can and do come from any of the other EU member states. This should not cause a major problem for the update of the course however, as the course manager (the author) will divide content amongst the trainers and all trainers will attend the upgrade meeting with their updated materials. The meeting will then provide a forum for discussion. The Moodle Course Management System (CMS) (Moodle.org, 2009), managed by University College Dublin, will also be used to get feedback regarding content updates before the meeting in October 2009.

A second issue is that all students are also international. Although the prerequisites state that it is essential that students have a good working knowledge of the English language, as the course lessons will be taught in English, there will inevitably be students with differing language skills. Particularly important is to ensure that colloquial English is not used. An online course may be much better in this respect as the content can be well thought out and phrased properly beforehand rather than a trainer giving an explanation spontaneously in a class-based situation.

Another problem unique to this course development is the differences in hardware between the distributed students. In the class-based course it was fairly easy to ensure that all students had the same or similar computer systems. This was especially important as Linux and some of the associated tools require particular hardware in order to run correctly. This could be a major issue as although the minimum specification of computer equipment will be defined there is a huge

scope for individual differences. Students will be encouraged to check hardware compatibility lists in particular UbuntuHCL.org (2009). Supporting hardware issues remotely will be challenging, however, it is intended that there will be a forum for discussion on the courseware site (again powered by Moodle). This discussion board will provide a way for students to attempt to solve each others problems as well as for tutor support. Students should also be able to contact tutors direct via email and perhaps Telephone or via Skype. Tutor availability may be an additional problem as all trainers are essentially volunteers with day jobs. In subsequent bids for funding it may be necessary to ask for financial support to cover the time the trainers spend online.

Hardware issues could cause other problems as some of the current class-based materials use floppy disk drives whilst others use USB devices. This can be solved by updating course materials to only cover USB devices (floppy drives are becoming less and less common since the introduction of higher capacity, smaller and safer USB thumb drives).

In addition to hardware issues, other software installation could cause problems. The easiest solution to this problem is to ensure a network connection and use the `apt-get` installation tool. Another solution would be to provide all the software libraries on the Moodle server.

By far the largest problem we foresee however is with the content itself. Linux is notoriously difficult to learn and to teach. Whilst the hardware support and user interface are much improved from the early days of the operating system, Linux simply does not quite work the way a Windows user expects. The Linux as a Forensic Tool course also makes extensive use of the command line interface with which most users will be unfamiliar. In an attempt to address this problem, similar online/distance learning courses will be looked at as well as some of the literature for converting a class-based course to an online/distance learning module.

The Analysis of Similar Online/Distance Learning Courses

The Open University, UK began teaching a distance-learning course called Computer Forensics and Investigations (CFI) containing some online elements in May 2008 (Open University, 2009). CFI is a postgraduate module with no face-to-face tuition, no laboratories, and no licensed software. The course is taught over a 24-week period (requiring around 6–8 hours per week of study). Due to the lack of a laboratory and licensed software, free and open source tools are used to teach the course. Both the tools and computer forensics techniques taught are therefore similar to those on the Linux as a Forensic Tool course. CFI is taught largely using printed materials with software and case study material supplied on CD. This is augmented with an online discussion forum and online assessment submission

procedures. The lack of a laboratory and no face-to-face teaching means that technical problems are difficult to deal with and support is provided via the online forum and limited telephone/e-mail support from tutors. In the first year of running, the attrition rate was around 35% and grades were amongst the lowest at the Open University. Possible explanations for this include the course being both technical (large elements of computing including Linux) and non-technical (essay and discussion based). Students that were more technical may have been put off by the non-technical aspects and vice versa. There also exists the possibility of poor teaching and/or poor course design (Price, 2008). For the Linux as a Forensic Tool course only the second of these suggestions poses a problem as students on the course will be serving police officers accustomed to dealing with both the technical and non-technical parts of the job. In terms of the suggestion of poor teaching and/or poor course design, the Open University is one of the largest organisations in the UK delivering distance education programmes and they have both stringent development procedures and strict staff hiring policies in place. It is difficult to believe therefore that this is the case. However, Price's results do suggest a careful handling of this subject matter and perhaps learning aids other than just printed materials.

Another example of digital forensics courses being taught online are those of Champlain College, USA. The BS in Computer & Digital Forensics has been offered at the college since 2003 (Champlain College, 2009). Both online and class-based versions of courses are offered. The content and the computer forensics techniques used by the course team are similar to those explored by the Linux as a Forensic Tool course. The difference between the Champlain College courses and that of the Open University course is in a greater use of the online technology in particular the use of the voice-over PowerPoint delivery of lecture method. In 2006, Champlain College performed a study to find out if the learning objectives of the computer forensics courses were being met equally well in both online and class-based courses. The results showed that while there was no significant difference between course outcomes in the two delivery modes, average grades in the online courses were slightly higher (Kessler, 2007).

Conversion of Class-based Content to Online/Distance Learning Material

nof-digitise Technical Advisory Service (no date) make some recommendations concerning the planning of online learning such as:

- the use of standards on the use of language, e.g., -ise versus -ize;
- learning design issues, e.g., learning objectives, overviews, summaries;
- content selection and length of sessions;
- target learners, e.g., knowing your audience.

These issues to a large extent were covered by the original course design team and as such the information exists in both the training materials and the Trainer's Guide and so will not be covered here. It is also probably worth mentioning that the development team has no intention of producing a HTML-only-based resource. Rather a series of learning objects that simulate the class-based experience will be made available via the Moodle CMS. These objects could also be distributed via CD/DVD.

At the moment the Linux as a Forensic Tool course consists of PowerPoint slides, which in a class-based scenario would be talked over and interspersed with demonstrations. There are exercise sheets which would be covered by in class demonstrations once students had had sufficient opportunity to attempt the task. There is reading material in the form of PDF documents, as well as a number of evidence files, some of them extremely large, for example, a Windows XP image file is 2.86GB.

To turn these materials into online/distance learning based content the course team propose enhancements to current content in a number of areas.

Voice-over-PowerPoint Presentations

These will be used for stand-alone lectures that do not require demonstrations. This will be achieved using PowerPoint's built in ability to record audio. The session will be scripted to ensure colloquial English is not used and that a common standard of language is used. According to Schneiderman (1992) (cited in Oliver, n.d.) online lectures need to be shorter and more to the point than traditional face-to-face sessions. This will mean carefully considering the length and content of each session accordingly. A transcript of the audio can also be provided for users without sound equipment and to improve accessibility.

Voice-over-screen Capture Presentations

For sessions that require demonstrations and possibly some element of PowerPoint, software such as Wink (2008) or Screentoaster (2009) will be used. Wink enables the user to create flash movies containing audio and text explanations. Screentoaster is an online service which allows the creation of QuickTime Video Clips. Both systems work under Linux and both produce content suitable for online download. Transcripts of any command line work can be produced using the Linux `script` command. These can then be appropriately colour coded by the development team to indicate the prompt, input and output.

Documents, Evidence Files and Software

Tutorial documents will be available as before however these may be accompanied by either video clips and/or reader documents so that a full explanation of their

purpose can be given. As evidence files and software are large it is proposed that all content is given to students both online and via removable media. This has the advantage of making the material immediately available to those without or with very slow network connections. However, if students are working away from their usual machines they can still access materials.

Other Online/Distance Learning Strategies

One aspect that will need to be taken into account is an introduction to the Moodle CMS will have to be given so that students understand how to use the system. This process could be used to engage the students early on in online discussion and collaboration. Although online/distance learning can be thought of as an asynchronous activity, Kessler (2007), Oliver (n.d.) and Mason (1998) all advocate synchronous activities to maintain student interest. One way of achieving this is by getting them involved in a discussion forum early. This can be maintained by getting students to post at regular intervals on particular topics. Student answers to exercises that are set can also be uploaded and answer sessions only posted when this happens, possibly with tailored class feedback. Contact details of tutors will obviously be available and the team is considering some notion of 'office hours' when staff will be available. Lastly, the online assessment activity can be set online and follow a similar pattern to some of the exercises set throughout the course.

Future Work

The first aspect of this work that will need to be completed is the actual upgrade of the Linux as a Forensic Tool course, including the inclusion of the online materials for the first week of the module. This process will allow the evaluation of some of the methods for converting to online content in terms of ease of use and time constraints for tutors. For example, evaluations of voice-over-PowerPoint versus Wink (2008) versus Screentoaster (2009) versus printed materials can then be made. The materials for the course will be finalised in October 2007 at the update meeting to be held at the Norwegian Police University College in Oslo.

The next step in the process will be the delivery of the content to students. The online element is pencilled in to occur between March and May 2010 followed by the class-based part between 7 and 11 June 2010. This will allow evaluations to be made and modifications to be suggested.

Lastly, the production of online materials for the Linux as a Forensic Tool course can be seen as a pilot for all ten courses developed by the expert group as a part of the MSc. If successful, then all other courses may at some point in the future be upgraded in a similar fashion and so any lessons learned will be invaluable.

Conclusions

This paper discusses the development of the Linux as a Forensic Tool course from its origins as part of the Falcone and AGIS projects through to its place in the ISEC funded MSc to be validated by University College Dublin. Of particular interest is the fact that half of this course is to be delivered using online/distance learning methods. There are several good reasons for developing computer forensics courses with this delivery method including cost savings and the lack of qualified staff and tutors. There are a number of unique issues raised by the development of the online/distance learning aspect of this course such as the international nature of the course (staff and students are distributed and have different levels of language skills), hardware and software issues, and most importantly the difficulty of the content itself. To try and make sure that the materials developed are of the desired quality similar online/distance courses developed by the Open University and Champlain College were studied. This study suggested that a range of online/distance learning strategies were preferable to a course booklet only approach. Instead, course materials will be provided online and on removable media which will consist of voice-over-PowerPoint, voice-over-screen capture, printed materials, evidence files, and software resources. In addition, a Moodle server will be used to promote group discussion and communication. Synchronous activities will also be organised to encourage student participation and enthusiasm. It is hoped that these methods will make for a successful module which could be used as a model for future online/distance learning computer forensics course developments.

References

Bennett, D., & Stephens, P. (2008, July). A usability analysis of Autopsy Forensic Browser. *Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008)*, University of Plymouth, UK.

Carrier, B. (2003). *Open source digital forensic tools: The legal argument* [online]. Retrieved June 21, 2008, from http://www.digitalevidence.org/papers/opensrc_legal.pdf

Champlain College. (2009). *Computer & digital forensics* [online]. Retrieved April 7, 2009, from http://digitalforensics.champlain.edu/

Childs, D., & Stephens, P. (2008, September). An analysis of the accuracy and usefulness of Vinetto, Pasco and Mork.pl. *Proceedings of the Second International Conference on Cybercrime Forensics Education & Training (CFET 2008)*. Canterbury Christ Church University, UK.

Eurim. (2004). *IPPR E-Crime Study drafted by UK MPs, Supplying the skills for justice: Addressing the needs of law enforcement and industry for investigatory and enforcement skills* [online]. Retrieved April 6, 2009, from http://www.eurim.org/consult/e-crime/may_04/ECS_DP3_Skills_040505_web.htm

European Commission. (2002). *Falcone — Helping people and organisations fight against organised crime at EU level* [online]. Retrieved April 6, 2009, from http://ec.europa.eu/justice_home/funding/expired/falcone/wai/funding_falcone_en.htm

European Commission. (2006). *AGIS was a framework programme to help police, the judiciary and professionals from the EU Member States and candidate countries co-operate in criminal matters and in the fight against crime* [online]. Retrieved February 10, 2009, from http://ec.europa.eu/justice_home/funding/2004_2007/agis/funding_agis_en.htm

European Commission. (2008). *Prevention of and fight against crime* [online]. Retrieved February 10, 2009, from http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm [Last accessed

Kessler, G. (2007, January). Online education in computer and digital forensics: A case study. *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS-40),* Hawaii.

Moodle.org. (2009). *Welcome to the Moodle Community* [online]. Retrieved April 7, 2009, from http://moodle.org/

NIST. (2008). *Welcome to the Computer Forensics Tool Testing (CFTT) Project web site.* [online]. Retrieved June 21, 2008, from http://www.cftt.nist.gov/

nof-digitise Technical Advisory Service. (n.d.). *Programme manual: Section 2. Creating online learning materials* [online]. Retrieved April 7, 2009, from http://www.ukoln.ac.uk/nof/support/manual/learning-materials/

Ó Ciárdhuain, S., Patel, A., & Gillen, P. (2003). *Training: Cyber crime investigation.* International Federation for Information Processing (IFIP) website [online]. Retrieved August 17, 2007, from http://www.ifip.org/TESTIFIP/WebPages/openbiblio/opac/viewDocument.php?id=92&PHPSESSID=f11c46e158952626dca6ddad9b509c60

Oliver, C. M. *Integrating online learning into your course* [online]. Retrieved April 7, 2009, http://www.alt.ac.uk/docs/eln064.pdf

Open University. (2009). *M889 – Computer Forensics and Investigations* [online]. Retrieved April 7, 2009, from http://www3.open.ac.uk/courses/bin/p12.dll?C01M889

Price, B. (2008). *Teaching computer forensics at a distance* [online]. Retrieved April 7, 2009, from http://www.ics.heacademy.ac.uk/events/presentations/727_Price-OU%20Computer%20Forensics-Glamorgan.ppt

Screentoaster. (2009). *Online screen recorder. Capture screencasts instantly* [online]. Retrieved April 7, 2009, from http://www.screentoaster.com/

Stephens, P., & Induruwa, A. (2007, August) Cybercrime investigation training and specialist education for the European Union. *Proceedings of the 2nd International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007), University of the Aegean, Samos, Greece.* IEEE Computer Society Press.

UbuntuHCL.org. (2009). *Ubuntu Linux hardware compatibility list* [online]. Retrieved April 7, 2009, from http://www.ubuntuhcl.org/

Wink. (2008). *Wink* [Homepage] [online]. Retrieved April 7, 2009, from http://www.debugmode.com/wink/