An Evaluation of Linux Cybercrime Forensics Courses for European Law Enforcement

P. Stephens

Department of Computing (Academic), Canterbury Christ Church University,
Canterbury, Kent, CT1 1QU, United Kingdom
e-mail: paul.stephens@canterbury.ac.uk

Abstract

This paper outlines models for the process of course selection and the development process used for producing the Linux as an Investigative Tool and Forensic Scripting Using Bash courses. These modules were developed as part of the ISEC 2008 Project, titled: "Developing and disseminating an accredited international training programme for the future". The two courses are part of an MSc accredited by University College Dublin. The evaluations of the two courses are included showing that the models presented for the course selection and development processes seem to be extremely helpful.

Keywords

Police, Linux, Cybercrime, Forensics, Courses, Evaluation

1 Introduction

This paper outlines a unique development of Linux cybercrime forensics courses for law enforcement practitioners. The design, delivery and evaluation of these courses was carried out by academics and forensic computing professionals from across the European Union with funding from the European Commission (2008a), Microsoft, An Garda Siochana, Landesamt für Ausbildung, Fortbildung und Personalangelegenheiten der Polizei NRW, and the National Policing Improvement Agency. The developers comprised law enforcement personnel from 18 member states, CEPOL, Europol, Interpol, and the UN ODC. In addition, developers from academia included lecturers from Canterbury Christ Church University, University College Dublin, and Universite de Technologie de Troyes. The process of course selection is highlighted in Figure 1, where project participants suggest and discuss new courses culminating in a vote for the most suitable suggestions. This ensures that both professional and academically relevant content is produced leading to accredited courses that are fit-for-purpose. The structure suggested is a modular one with courses at basic, intermediate, advanced and CPD levels.

These courses were part of an MSc in Forensic Computing and Cybercrime Investigation accredited by University College Dublin. This paper discusses two courses for which the author was the course manager and lead trainer: *Linux as an Investigative Tool* and *Forensic Scripting Using Bash*. Before the evaluations of

these courses are discussed however it is worth noting how the courses were developed.

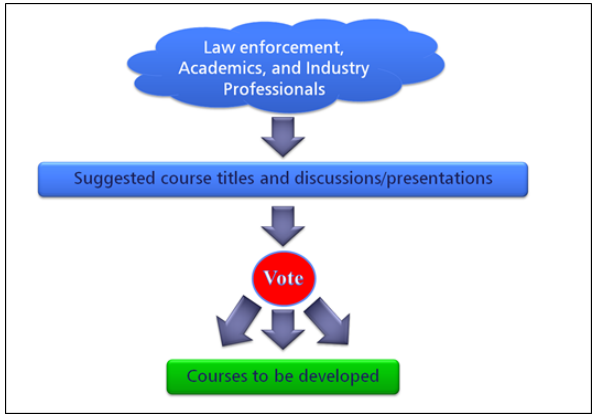

Figure 1: Process of course selection

2 Development Process for the Linux Cybercrime Forensics Courses

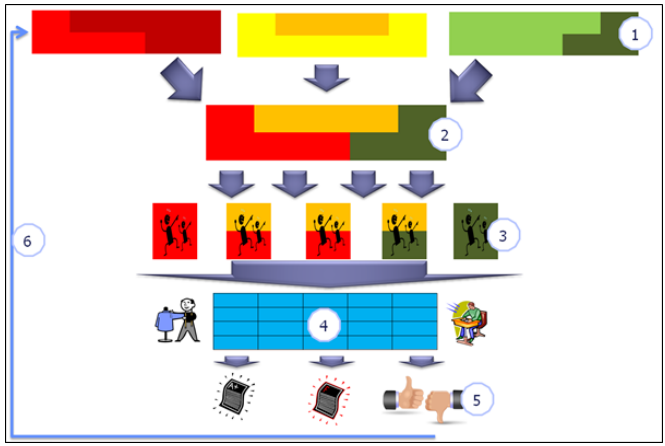

Figure 2: Management Process for Individual Course Development

Figure 2 shows how the development process was managed. **1** Shows how individuals come to the planning meetings with their own courses, ideas for courses and preparatory work. **2** Shows how the courses, ideas and preparatory work are combined to make a coherent timetable. **3** Shows how the content is then given to a presenter to develop and a seconder for checking. Presenters are responsible for content but the syllabus has already been defined in **1** and **2**. At **4** the training designer and course manager okay the final timetable for presentation to students and

then the course is run. **5** The course is assessed and evaluated. **6** These outcomes are fed back into future runs and/or upgrades of the course. This model evolved over a number of years through a number of similar development projects funded mainly by the Agis Programme (European Commission, 2008b). One of the elements that was added following the pilot run of the Linux as an Investigative Tool course was the addition of the seconder, not only to check over materials developed by a presenter, but also to support the students in the classroom. Up until this point the other three or four trainers who were not presenting were expected to support students, however, due to the complexity of the subject not all trainers were familiar enough with the content to do this in any meaningful way.

The Linux as an Investigative 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 (see Carthy et al. (2007)). The first week would cover the basics of Linux in a forensic computing context. Week two would cover the more in depth forensic features of Linux and the associated tools. The timetable for the first week of the course is shown in Figure 3.

Monday	1.1 Course Opening	1.2 Introduction and installation of Linux	L	1.2 (cont'd) Introduction and installation of Linux	1.3 Self reflection
Tuesday	2.1 Review of previous day	2.2 Basic Linux commands	U	2.2 (cont'd) Basic Linux commands	2.3 Self reflection
Wednesday	3.1 Review of previous day	3.2 Standard Linux Tools	N	3.3 Standard Linux Tools - System Admin Perspective	3.4 Self reflection
Thursday	4.1 Review of previous day	4.2 Standard Linux Tools - Working with Hashes	C	4.3 Week 1 Course Review	4.4 Self reflection
Friday	**5.1 Assessment**	5.2 Course Evaluation and Next Steps	H	5.3 Tutorials	

Figure 3: Timetable for week one of Linux as an Investigative Tool Course following evaluations

Following this week the recommendation was that students of the course would need one to two months for the material to sink in and to work on related tasks. Therefore the following tasks were outlined as homework:

- Step One: Work through week one's materials and exercises;
- Step Two: Work through tutorial material; and

- Step Three: Brush up on file systems knowledge.

This would be followed by week two of the course as outline in Figure 4.

Monday	**6.1 Course Opening and Assessment**	6.2 Forensic file formats		L	6.3 String search with egrep	6.4 Information gathering and acquisition tools	6.5 Self reflection
Tuesday	7.1 Review of previous day	7.2 Evidence acquisition tools Keyword search		U N	7.3 Use of the file system Undelete files	7.4 Timeline File headers Finding pictures Metadata in pictures	7.5 Self reflection
Wednesday	8.1 Review of previous day	8.2 Scripts basics Thumbnails Video analysing	8.3 Salvage - carving Windows registry	C	8.4 NTFS compression and encryption MS Office documents Windows password cracking	8.5 Anti-Forensics	8.6 Self reflection
Thursday	9.1 Course Review	**9.2 Assessment**	9.3 Course Evaluation and Closure	H	9.4 Tutorials		

Figure 4: Timetable for week two of Linux as an Investigative Tool Course following evaluations

3 Linux as an Investigative Tool Evaluation

The online element of the course (the development of which is discussed in more detail in Stephens (2009)) was carried out between March and May 2010 and the class-based part was delivered at the Hellenic Police Academy, Veria, Greece in June 2010. There were 28 students from law enforcement agencies across the European Union enrolled on the MSc in Forensic Computing and Cybercrime Investigation accredited by University College Dublin. The students had a range of experience from less than two years to more than fifteen, however all students had attended the previous MSc level courses on Introductory IT Forensics and Network Investigations, Applied NTFS Forensics, Intermediate Internet Investigations, and Intermediate Network Investigations. Less than half the class had any experience of using Linux and less than 20% had used Linux for forensic investigations. All courses on the MSc dealt with differences in practice between member states by focussing on the IOCE (2012) G8 Proposed Principles For The Procedures Relating To Digital Evidence. Provision was also made for students to discuss local variations in practice and legislation in classes with other students and trainers.

Formal evaluation of the MSc run of the Linux as an Investigative Tool took place using the Kirkpatrick Model (Kirkpatrick and Kirkpatrick, 2006) Level 1, Level 2 and Level 3 (previously a pilot of this course had run and was evaluated in Carthy et al. (2007)). Level 1 involves gauging student reaction to the course using student feedback (commonly referred to as 'happy sheets'). In the case of the online element

of the course participants completed an end of online course questionnaire on the SurveyMonkey website (SurveyMonkey, 2011). For the in class element of the course, participants completed daily questionnaires on SurveyMonkey. The SurveyMonkey questionnaires provided qualitative and quantitative data. The frequency of feedback made it easier for the trainers to react to any problems that were identified. For example, if students experienced difficulties with a particular element then during recaps more time could be spent on this area. Exercises were also adjusted in line with feedback. Kirkpatrick Model Level 2 involves attempting to assess the extent to which student learning has taken place. The course knowledge assessment/examination acted as this Level 2 independent evaluation of the extent to which course learning objectives were met by the students. The Level 3 evaluation involves asking managers of the students on the MSc to comment on how the programme has affected their working capability and practice. In addition to these Kirkpatrick evaluations, students completed a learning journal for the MSc and an exit interview was conducted by members of the project team.

Student feedback was generally very positive (see Figure 5 for the Aggregate Rating for Overall Session Grading); however, some students struggled with the content including two students, out of the 28 that sat the course, failing the assessed elements. This was despite adding an extra day at the beginning to the class-based part of the course to review work covered by an online part of the module. Overall the student average was 80%. All students passed the assessed elements on resit.

As can be seen from Figure 5, approximately 1% of participants rated any of the sessions as very poor. This equates to only three out of 520 responses overall, restricted to only three sessions. Approximately 1% of participants rated any of the sessions poor. This equates to only eight out of 520 responses overall, restricted to six sessions. Interestingly there is only an overlap between poor and very poor responses for two sessions. Where sessions were rated poor or very poor, comments indicate that students found it difficult to keep up as there seemed to be a lot of material in these sessions. For future runs of the course the materials and the evaluations will be available to trainers so that they can make changes, if they deem it necessary.

Some students believed that the standard of the training equipment could have been improved but on the whole comments were positive. Particular highlights for the students included conversion between forensic file formats, regular expressions and the level of detail covered in describing commands and their switches.

Student quotes directly related to this course include:

> "The course itself was excellently presented, I found the subject matter fascinating, and I am utilising my knowledge in the workplace already. I have spent the last few days stripping out IP/time data from a 900MB text document containing compromised data using Linux, … it is most definitely not something I could have achieved prior to this course."

and

> "I have learned to convert a DD image to another evidence file format to suit the tools I'm using such as EnCase. This is only one example of how what I have learned can be used to my advantage, other examples include extracting metadata from images and using the file system to undelete files."

These are encouraging as both examples point to ways in which their investigative practice has been improved carrying out tasks that would not have been possible without this training. Managers' feedback for the MSc as a whole was also positive and encouraging.

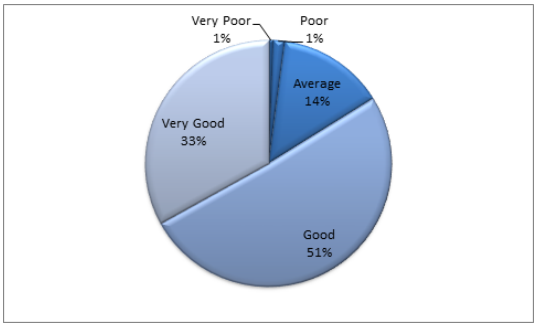

Figure 5: Aggregate Rating for Overall Session Grading for MSc run of Linux as an Investigative Tool

4 Forensic Scripting Using Bash Evaluation

The pilot of the Forensic Scripting Using Bash course ran in April 2010 at the National Police Training Centre, Madrid, Spain. Students for this course were again drawn from the European Union law enforcement community but were not studying on the full MSc programme. There was a pre-course assessment that all students had to take to test their knowledge of Linux before the course. This was necessary as the module was meant to fit into a master's degree program where students had studied Linux forensics to sufficient depth. None of the students on the course in Madrid had previously studied the Linux as an Investigative Tool course and therefore the test was used as a way of judging whether or not students had the equivalent knowledge required. Approximately one-third of students failed the pre-course assessment and five (out of 20) students went on to fail the course assessment at the end. The pre-course assessment was therefore indicative of the number of students that would fail the course. The ISEC 2008 MSc Programme Evaluation Report makes it clear that the pilot of the Forensic Scripting Using Bash course suffered due to some of the students not meeting the pre-requisites specified. In the future students should have either passed the Linux as an Investigative Tool module first or must pass a pre-course assessment. Student feedback was generally very positive (see Figure 6 for the Aggregate Rating for Overall Session Grading); however, there

was a recommendation that the session at the end of the course be made optional or removed as students found it difficult to concentrate following a test. Overall the student average was 58%. Figure 6 As shows that no participant rated the sessions very poor and the poor ratings refer to only six out of 329 responses overall, restricted to only four sessions. One of these sessions (Beyond Bash) was removed due to this feedback. The other sessions either did not receive any relevant comments or referred to difficulties in understanding language or the session being 'slow'. The timetable in Figure 7 gives an indication of the content of the course.

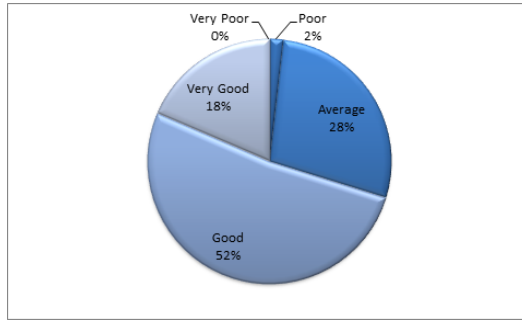

Figure 6: Aggregate Rating for Overall Session Grading for Pilot of Forensic Scripting Using Bash

Monday	1.1 Course Opening	1.2 Introduction to Developing Software and Shell Scripting		L	1.3 Making Decisions (if and case constructs)	1.4 Self reflection
Tuesday	2.1 Review of previous day	2.2 Repeating Sequences (while, until, and for constructs)		U	2.3 Utilities, Functions, Testing, and Debugging	2.4 Self reflection
Wednesday	3.1 Review of previous day	3.2 Forensic Case Studies using the Linux as a Forensic Tool Course examples		N	3.3 Forensic Case Studies using Grundy examples	3.4 Self reflection
Thursday	4.1 Review of previous day	4.2 Enhancing the User Interface and Improving Output		C	4.3 Further Forensic Scripting (using Linux as a Forensic Tool Course examples?)	4.4 Self reflection
Friday	5.1 Course Review	**5.2 Assessment**	5.3 Course Evaluation and Closure	H	5.4 Beyond bash (not assessed)	

Figure 7: Timetable for Forensic Scripting Using Bash Course

The course ran as part of the MSc (with the same students as outlined in section 3 above) in September 2010 at University College Dublin, Ireland. All students on this course had sat the Linux as an Investigative Tool Course (although two had failed the final assessment). Again student feedback was very positive (see Figure 8 for the Aggregate Rating for the Structure and Method of Delivery for the MSc Run of Forensic Scripting Using Bash and Figure 9 for the Aggregate Rating for the Level of Student Understanding for the MSc Run of Forensic Scripting Using Bash), however five students out of 28 failed the end of course assessment worth 50%, however, these students have since passed on resit. The overall student average for the test element was 68%. All students passed the other 50% element for which the average mark was 78%.

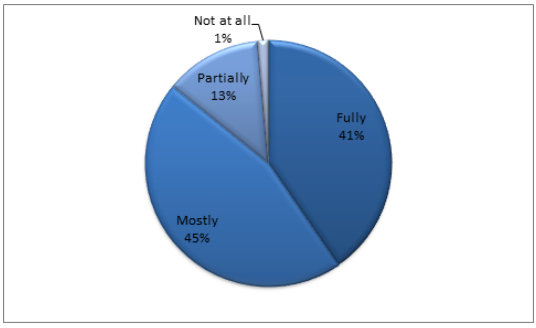

Figure 8: Aggregate Rating for the Structure and Method of Delivery for the MSc Run of Forensic Scripting Using Bash

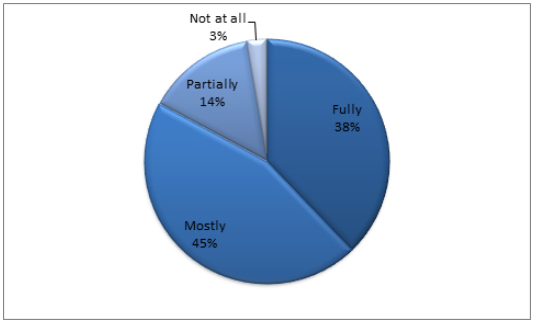

Figure 9: Aggregate Rating for the Level of Student Understanding for the MSc Run of Forensic Scripting Using Bash

Some students were concerned about the difficulty of the subject matter. It is worth noting that trainers put a lot of work into the course including outside of the classroom as shown by the following comment:

> "Working through the exercises in the evening is very beneficial as is the availability of the trainers for that time. Much appreciated."

Student quotes from the learning journals that are particularly relevant to the Forensic Scripting Using Bash course are:

> "The web spider we have learnt is incredibly valuable for our work of monitoring…websites. We were highly surprised when we saw how easy is with a non very long script, to have a real time monitoring system to display all the changes in a website"
>
> and:
>
> "From a confidence point of view, the last few 'Linux' months, and in particular the scripting course and post-course assignment, having proven to be invaluable. … Over the last three years, I have been constantly mindful of the expertise that surrounds me, the knowledge that my colleagues have acquired over many years of hard work, and for which I feel I can only ever aspire to. Having completed my script, I was asked by two of the most experienced colleagues if I would provide them with a copy of my script, as they wished to look at it and learn from it. I am still in shock that I am seen as somewhat of a relative 'expert' on this subject!"

Again, these are encouraging as both examples point to ways in which their investigative practice has been improved carrying out tasks that would not have been possible without this training. One particularly pertinent manager's response is:

> "has also developed different useful forensics tools and software packages that are used by all members of the unit."

This response shows that the programming elements have really paid off for this particular student and their workplace. For future runs of the course the materials and the evaluations will be available to trainers so that they can make changes, if they deem it necessary.

5 Conclusions

This paper has presented models for the processes of course selection and management for a pan-European, joint venture between law enforcement and academia that may be useful for other professional and academic course development collaborations. In addition, two courses have been evaluated using the Kirkpatrick Model, student learning journals and course exit interviews. The results of these evaluations were highly encouraging, suggesting that the process and management models could be reused in the future.

6 References

Carthy, J., O'Reilly, D., Gillen, P., and Stevens, T. (Eds.) (2007) *Cybercrime Investigation – Developing an international training programme for the future (Phase 4)*, AGIS PROGRAMME JLS/2006/AGIS/010. Wyboston: National Policing Improvement Agency (NPIA).

European Commission (2008a) *Prevention of and Fight against Crime* [online]. Available at: http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm [Last accessed 21 June 2008].

European Commission (2008b) *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]. Available at: http://ec.europa.eu/justice_home/funding/2004_2007/agis/funding_agis_en.htm [Last accessed 21 June 2008].

IOCE (2012) *G8 Proposed Principles For The Procedures Relating To Digital Evidence* [online]. Available at: http://www.ioce.org/core.php?ID=5 [Last accessed 27 April 2012].

Kirkpatrick, D.L. and Kirkpatrick, J.D. (2006). *Evaluating Training Programs: The Four Levels (3rd Edition)*. San Francisco, CA: Berrett-Koehler.

Stephens, P. (2009) 'Teaching 'Linux as a Forensic Tool' (Online) to European Law Enforcement'. *Readings in Technology and Education: Proceedings of ICICTE 2009*, Corfu, Greece, July 9-11, 2009. ISBN: 1-895802-42-3.

SurveyMonkey (2011) *SurveyMonkey: Free online survey software & questionnaire tool* [online]. Available at: http://www.surveymonkey.com/ [Last accessed: 7 February 2011].