2010

Development, Delivery and Dynamics of a Digital Forensics Subject

Tanveer A. Zia
Charles Sturt University

DOI: 10.4225/75/57b2b78240ce6
Originally published in the Proceedings of the 8th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, November 30th 2010

Development, Delivery and Dynamics of a Digital Forensics Subject

Tanveer A Zia
School of Computing and Mathematics
Charles Sturt University
NSW, Australia
tzia@csu.edu.au

Abstract

Digital forensics is a newly developed subject offered at Charles Sturt University (CSU). This subject serves as one of the core subjects for Master of Information Systems Security (Digital Forensics stream) course. The subject covers the legislative, regulatory, and technical aspects of digital forensics. The modules provide students detailed knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools, e-evidence collection and preservation, investigating operating systems and file systems, network forensics, email and web forensics, presenting reports and testimony as an expert witness. This paper summarises the process of subject development, delivery, assessments, teaching critique, and provides results from online subject evaluation survey. The dynamics and reflection on subject delivery is particularly important to determine if the subject has met its objectives. Results from the subject critique and student evaluation survey are presented and a reflection on how to improve the subject is provided.

Keywords

Forensics education, digital forensics subject, computer forensics course, forensics teaching and training.

INTRODUCTION

Digital Forensics is the field of forensics science that deals with digital crimes and crimes involving computers. Digital forensics is emerging as an important field of study in Information and Communication Technology (ICT) security as well as in advance law studies. Due to the fact that modern society is becoming more and more digital commercially and socially, the field of digital forensics is taking a focal point in legal world as well as the technical world (Landman, 2002). Digital forensics is used not only to investigate computerised crimes, such as network intrusion, fabrication of data and illegitimate material distribution through digital services, but also to investigate crime where evidence is stored in any digital format on any digital device. Given the importance and sensitivity of digital forensics discipline it is vital to design a subject which equips our ICT security graduates with advance forensics knowledge both technically and conceptually. This paper not only presents a new digital forensics subject and its delivery but also provides the reflection as result of teaching critique and a subject evaluation survey completed at the end of the teaching session.

The process to develop the new digital forensics subject at Charles Sturt University was initiated in consultation with industry experts in early 2009. This resulted the development of a new subject called ‘Digital Forensics’. This subject is one of the core subjects offered in Master of Information Systems Security – Digital Forensics stream, a course offered by the School of Computing and Mathematics. The author has the privilege to write, compile, coordinate, teach, assess and reflect on the subject which was offered in Session 1, 2010 for the first time and has been well received by the students with 43 enrolments in the first offering. The unique aspects of this subject are its applied approach. Weekly modules and assessments are designed in such a way that experienced learners can reflect on their real-life forensics experience and novice learners can gain valuable knowledge which will be applied when they embark on a forensics career.

Students have particularly appreciated the hands-on projects because of interactive nature which provides a real life forensics investigation experience. Below is the subject description and objectives taken from the Subject Profile:

This subject provides an in-depth study of the rapidly changing and fascinating field of computer forensics. It combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes. Upon successful completion of this subject, students should:

- be able to argue the legal and ethical considerations for investigating and prosecuting digital crimes;

- be able to develop a digital forensics process;
- be able to select and evaluate the technology in digital forensics to detect, prevent and recover from digital crimes;
- be able to analyse the storage media and file systems;
- be able to collect electronic evidence without compromising the original data;
- be able to evaluate the functions and features of digital forensics equipment and the environment and the tools for a digital forensics lab;
- be able to identify technical tactics used in the preparation and planning of digital crimes and the cybertrails they leave;
- be able to analyse the steps involved in a digital forensics investigation and to prepare reports on the results of investigations.

The rest of the paper is organised as follows. Section 2 presents the subject development process which includes rationale behind choosing the textbook, recommended readings and outlines the subject content. Subject delivery and teaching is discussed in Section 3. Section 4 summarises the assessments. Section 5 discusses the dynamics, critique and student survey evaluation results. Finally the paper is concluded in Section 6.

SUBJECT DEVELOPMENT

The subject is developed in close consultation with the industry experts and lawyers who are involved with handling the digital forensics cases as part of their professional practice. In any subject, having a textbook as a primary source of reference is important. Due to the emerging nature of the digital forensics discipline it is very challenging to find all the contents in one book. Especially, books written in Australian context are rare. With careful consideration (Nelson, Phillips, & Steuart, 2010) is used as a textbook in conjunction with several recommended readings (Wright, 2009; Newman, 2007; Slay and Koronios, 2006; Carrier, 2005; Vacca, 2005; Volonino, Anzaldua, and Godwin, 2007; Britz, 2009). The subject contents in following section are derived from the prescribed textbook and recommended readings.

Topic 1: Understanding digital forensics and digital detective

This topic defines digital forensics and describes how to prepare for digital investigations. It also describes the role of a digital forensics investigator. Students also learn the requirements to establish a digital forensic lab.

Topic 2: Digital forensics: legislations and code of ethics

Topic 2 examines the legal, regulatory and ethical concerns with the information security in general and digital forensics specifically. The topic also explains the incident handling and response process, evidence preservation, digital forensics and fact finding.

Topic 3: Digital crime: civil and crime law

This topic describes digital crimes and the legislations relevant to the use and misuse of digital devices. Issues evolving into civil and crime law are addressed. The topic also examines the ethical and legal principles that govern the behaviour of computer users.

Topic 4: Forensics process, policies, and procedures

This topic explains digital investigation process. Students learn how to prepare a digital investigation and apply a systematic approach to an investigation. The topic describes the procedures for a high-tech investigation. The topic also explains how to complete and critique a case.

Topic 5: Data acquisition and validation

This topic is about the digital evidence storage formats and how to determine best data acquisition methods using various acquisition tools. Students learn about the hashing algorithms used in forensics analysis to validate data. They also learn how to refine and modify the investigation plan, use data analysis tools and practices to process digital evidence, determine whether data-hiding techniques have been used, and learn methods for performing a remote acquisition.

Topic 6: E-Evidence, guidelines and standards

This topic teaches students how to process a digital investigation scene. Evidence rules are critical, whether investigating a corporate or a criminal case. Sometimes, a civil case can quickly become a criminal case, and a criminal case can revert to a civil case. Although this topic examines rules of evidence in the United States, but the procedures apply in most courts worldwide.

Topic 7: E-Discovery, tools, environments and equipments

Topic 7 explains how to evaluate needs for computer forensics tools. Students review several available computer forensics tools. This topic also lists some considerations for computer forensics hardware tools. Finally, students learn various methods for validating and testing these tools.

Topic 8: Investigating operation systems and analysing file systems

This topic reviews how data is stored and managed in operating systems (OSs). To become proficient in recovering data for computer investigations, students understand file systems and their OSs, including legacy (MS-DOS, Windows 9x, and Windows Me, for example) and current OSs, such as UNIX, Linux, Microsoft Windows 2000, XP, and Vista. In addition, this topic discusses media and hardware, such as CDs and DVDs and IDE, SCSI, and SATA drives.

Topic 9: Network forensics and intrusion detection

Topic 9 provides an overview of network forensics. Tracing network forensics information can take long, tedious hours of work, but this field overlaps digital forensics in many areas. This topic extends an idea of how digital and network forensics complements each other.

Topic 10: Email, handheld devices and web forensics

This topic explains how to trace, recover, and analyse e-mail messages by using forensics tools designed for investigating e-mail and general-purpose tools, such as disk editors. Over the past decade, e-mail has become a primary means of communication, and most computer users have e-mail programs to receive, send, and manage e-mail. Students also learn how to recover deleted e-mail from a client computer, regardless of the e-mail program used, and how to trace an e-mail back to the sender. In addition, students also learn how to obtain information from a mobile phone or hand held device.

Topic 11: Reporting and presenting

Topic 11 provides guidelines on writing reports of findings in digital forensics investigations. Students learn about different types of reports and what to include in a typical report. Students also examine how to generate report findings with forensics software tools. In addition, they learn the rules of evidence and procedure as they apply to testimony. Students learn about the types of testimony—for trials, depositions, and hearings—and the difference between a technical/scientific witness and an expert witness.

Topic 12: Expert witness and forensics accounting

For digital forensics examiners, maintaining the highest level of ethical behaviour in their work is essential. In this topic, students learn how computer forensics experts and other professionals apply ethics and codes of conduct to their work and to giving expert testimony. Digital forensics examiners are responsible for meeting the highest standards when conducting examinations, preparing reports, and giving testimony to ensure that evidence is accurate, reliable, and impartial. In addition, students discover the use of forensic techniques in investigating and prosecuting accounting fraud and other white-collar crimes.

SUBJECT DELIVERY

The subject is delivered in distance mode with the use of CSU Interact and WebEx training sessions. CSU Interact is an integrated online learning environment which allows staff and students to access a number of online services as well as several new teaching and learning tools. WebEx is a collection of real-time web conferencing services developed by WebEx Communications Inc., acquired by networking giant Cisco Systems. WebEx Training Centre has become a popular service for online delivery of education/training to distance students.

CSU Interact Modules tool is used to deliver weekly topics. The Modules tool is a lesson builder tool that allows subject coordinators to publish learning sequences that can be created by using a choice of built-in online editing functions. Each topic in a module contained weekly learning objectives, activities, short quizzes, weekly questions and some useful links. The Resources and Forum tools in CSU Interact were frequently used. Lecture slides and other learning material were made available in Resources. Students used Forum to stimulate discussion on their weekly learning. Forum was also helpful to seek help from the fellow students as well as the subject coordinator.

Through the teaching period of 12 weeks, six WebEx sessions were conducted fortnightly on Wednesdays at 8:00pm to 9:00pm. The choice of the day and time was in consultation with students. This is to allow working students finish their work and join the training sessions to increase students' participation. All WebEx sessions were recorded and recording was made available for later downloading or to those who have missed the session.

One of the interactive features of WebEx training tool is that it allows students to see the presenter/lecturer on their computer screens provided they have the audio/visual facility enabled. The presenter can present the lecture slides, use their desktop as a white board to illustrate or write something, and engage students in discussion. Students can also ask real-time questions either on their microphones or by typing in a chat window. Another very useful WebEx feature which was used in this subject delivery was the test centre. At the end of some teaching sessions a test was delivered to determine students understanding of the forensics concepts being delivered.

ASSESSMENTS

There are four assessment items with several tasks each in this subject. Assessment-1 which is due at the end of the session is to maintain a professional journal of digital forensics learning throughout the semester as well as maintaining and commenting on weekly blogs. Assessment-2 includes hands-on projects, a case project and a research project. Assessment-3 also has hands-on projects, a research question and a case study. Assessment-4 is an online exam containing multiple choice and short-answer questions.

Assessment-1: Professional Journal and weekly blogs

Assessment-1 is an on-going task of maintaining a professional journal and developing and maintaining a blog of learning activities. This assessment starts in first teaching week and continues until the last week. In this assessment students are asked to build and maintain a professional journal of digital forensics learning. Students are asked to join at least three electronic mailing lists and read them regularly. The mailing lists are about operating systems, user groups, forensics cases or forensics tools. The choice of mailing list is entirely up to the students.

Another task in this assessment is to maintain a blog using CSU Interact blog tool. Students are asked to post at least one blog entry every week and make a comment on at least one other blog entry of one of their peers.

The objective of this assessment is to have students demonstrate their ability to establish a journal/diary of digital forensics learning activities, communicate their activities in a blog, understand and comment on similar activities of their peers.

This assessment is marked against the following marking criteria:

- detail and completeness of the professional journal
- currency and relevance of activities listed in the journal
- the relevance and accuracy of the blog entries
- expression of ideas and concepts
- posting weekly blog entries
- reflection and review of the blog entries.

Assessment 2 and 3: Hands-on projects, case studies and research questions

These assessments contain some selected hands-on projects form the textbook. Some of these projects required students to use WinHex, Helix, EnCase, AccessData FTK and ProDiscover tools to perform most digital forensics acquisition and analysis functions.

Hands-on projects are vital in this subject. The rationale for this assessment is to enable students to complete important hands-on projects, solve case projects, investigate important forensics utilities, effectively use forensics tools, investigate file systems, and be able to write a case study based on their experience or learning in the subject. One of the challenging tasks in assessment 3 is an exercise. In this exercise, students are given a text file with scrambled bits and asked to restore the scrambled bits to their original order. This assessment task is important in this subject to give an aspect of real life scenario where a digital investigator has to reveal the evidence from concealed information.

The marking criteria in these assessments depend on:

- Successful completion of the hands-on projects
- Reflection on any difficulties faced in hands-on projects
- Relevance and accuracy of the solution to the Case project
- Detail of research conducted and references used in the Research project.
- Correct use of citations and referencing conforming to APA referencing format.

Assessment 4: Final Examination

The final examination is an online closed book examination which covers the entire subject syllabus. CSU has an exclusive arrangement with Prometric Testing Centres to conduct examination for most of the subjects offered in distance mode. The two hours examination consists of 20 multiple choice questions and five short answer questions. Marks are awarded against the accurate expression of ideas and demonstration of understanding of subject objectives, facts and concepts learned.

In order to pass the subject, a student must achieve a mark of 50% in both the overall mark and the final examination (Assessement-4). The percentage value of each assessment item is given in Table 1.

Table 1. Assessment tasks, value, delivery and feedback

Assessment tasks	Value	Due	Feedback returned
Assessment-1	20%	Week 12	Not returned
Assessment-2	20%	Week 6	Week 8
Assessment-3	20%	Week 10	Week 12
Assessment-4	40%	Week 13-14	Not returned

TEACHING CRITIQUE AND DYNAMICS

A teaching critique was conducted through a peer review process to comment on the online delivery of the subject. Below are the good practices recognised in the teaching critique report and recommended enhancements.

Good practices recognised:

- Frequent use of WebEx sessions and Forum which encourages students' participation to gain deeper knowledge
- Recording and availability of WebEx sessions for later student access
- Use of Forum was effective especially with assignment clarification
- The use of question-based learning blog/journal in the assignment enabled students to participate actively
- Activities and assignments had an applied approach which benefited the students in a real-time working environment
- Weekly activities, quizzes and questions provided students the opportunity to participate through the duration of the subject which enhanced their learning
- The module activities were directly related to the assessment schedule and real life experiences of a digital forensics specialist.

Recommended enhancements:

- Create sub-forums for each module to allow module-specific communication
- Develop assessment rubrics to make the expectations of the task more transparent
- Provide feedback on module activities to enable students to further participate and to ensure they are on the right track
- Advise students about the technical requirements in advance of the commencement of the subject.

EVALUATION FEEDBACK

Students have particularly liked the forensics stream and the technical aspects of the subject. With active participation on the discussion Forum and WebEx sessions, students were keen to learn this emerging area of study. Many students were from the background where they are involved in a profession relating to digital forensics. At the end of the session, an online subject evaluation survey was conducted. 19 out of 43 students completed the survey which is a good response rate of 44%. Overall mean is 5.62 (out of 7) which is very encouraging. The students have responded well to and appreciated the use of technology in learning. Students have particularly liked WebEx sessions, timely feedback on assessments, prompt responses to the Forum postings and emails, up-to-date concepts in the subject, and frequent use of Interact tools such as Blogs, Wiki, Chat, and Modules.

REFLECTION

Some hands-on projects required use of digital forensics tools to be installed on computers/laptops. Some students faced problems making those tools work due to variations in operating systems and technical configurations on individual's computers.

Reflecting on survey results and feedback from the students, following review is planned for future offering of the subject.

- Replace Reading 1 with a readily available publication in forensics law from Australian perspectives
- Delete the blog activity which seems to be time intensive and include the Professional Journal into one of the other 2 assessments
- Keep the assessment items to only three - two assignments and an end of session examination
- Include guidelines for the software tools needed to complete the hands-on projects
- Emphasise on the technical aspects of the subject more elaborately

It is anticipated that with these planned changes in future subject offering which will be Session 1, 2011, the subject can gain more popularity and may become a model subject in digital forensics teaching in a postgraduate level course.

DISCUSSION AND ANALYSIS

This paper began with introduction to the digital forensics as an important field of forensics science. Advancements in information technology have posed new challenges for policing the use of technology. 41% respondents of CSI Computer Crime and Security Survey (2008) have used forensics tools as part of the security technologies to detect and deter threats to information assets. In this paper need for a digital forensics subject is realised as a core subject in an information security course. Starting with the process of subject development, selecting the textbook and required readings, delivery of the contents particularly in distance mode, assessments and rational for assessment tasks and finally the evaluation of the subject through student survey and peer review are the notable aspects in this paper. While developing the subject contents, particular attention is paid on the four key elements of forensic computing identified by McKemmish (1999) at the Australian Institute of Criminology: (a) the identification of digital evidence (b) the preservation of digital evidence (c) the analysis of digital evidence, and (d) the presentation of digital evidence. Objective one of the subject provides awareness of Australian legal system and ethical considerations for investigating digital crimes. Objectives two and three correspond to the development of digital forensics process and technology to identify the digital evidence. Objectives four and five deal with the preservation and analysis of digital evidence in it original form. Objective six looks at the tools and equipment for a forensics lab. Objectives seven and eight focus on planning for digital investigation and presentation of evidence in a due process.

The rationale behind the use of the technology in subject delivery is primarily the audience which are geographically dispersed and mostly working professionals. The choice of two tools CSU Interact and WebEx is the ability of these tools to deliver the contents interactively reducing the need for a face to face contact. As mentioned in Section 3, these tools are purpose built lesson builder tools designed for a learning environment.

The approach in this subject is practical and real application of forensics scenarios. Assessments were designed to address this approach. The major tasks in the assessments were hands-on projects, real-life forensics case studies and demonstration of documenting the forensics processing by maintaining a professional journal throughout the session. The software and tools used in hands-on projects are the same as used in real life forensics labs such as: PitPim, Ethereal, Helix, HexWorkshop, WinHex, IrfanView, Knoppix STD, Sleuth Kit, S-Tools4, EnCase, AccessData FTK. Most of these tools are downloadable from the Internet as freeware, shareware, or free demo versions. A real challenges to assess students ability to reveal hidden evidence was the exercise of providing a text file with scrambled bits and asking students to restore to its original order.

Teaching critique and the evaluation survey provided valuable feedback to improve the subject. The teaching aspects which were explored in the critique were: design for learning, alignment with the subject objectives, learner engagement, learning context, learner extension, practice for learners, integration and technology suitability. Students' response to the subject evaluation survey was good with nearly half of the cohort completing the survey. The subject scored a mean of 5.62 out of 7 which is comparatively better than the School mean of 5.20 for all other distance subjects taught at the School in that session. Some of the most appreciable aspects of the subjects are the choice of textbook, learning material, access to online resources, use of online teaching tools and on time feedback on assessments.

CONCLUSION

Education in ICT security has become popular due to digitisation in every field of life. The increasing use of online social networks and digital devices which carry enormous amount of digital data requires stronger protection of digital information. This paper has presented a new subject in digital forensics with a major focus on principles and practices in ICT security, digital crime and investigation. It is anticipated that this subject will become a model subject in digital forensics and would lead to development of a new course in digital forensics.

To enhance the digital forensics subject we need to regularly review contents related to advances in legislations and technical developments. We also need to introduce new hands-on projects, latest hardware and software tools to improve the technical experience, develop active learning activities as well as emphasise the importance of enhancing the digital forensics as a discipline.

REFERENCES

Britz, M. T. (2009). Processing of evidence and report preparation. In Computer Forensics and Cyber Crime: An introduction, 2/e. Upper Saddle River, NJ. Pearson Prentice Hall

Carrier, B. (2005). File System Analysis. In File System Forensic Analysis (pp. 173-210). Upper Saddle River, NJ. Pearson Education Vacca, J. R. (2005). Evidence Collection and Data Seizure. In Computer Forensics, 2/e (pp. 217-233). Hingham, MA. Charles River M

Cisco WebEx (n.d.). Retrieved from http://www.webex.com.au/

CSI Computer Crime and Security Survey. (2008). Computer Security Institute. Retrieved from http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf

CSU Interact (n.d.) Retrieved from http://www.csu.edu.au/division/landt/interact/interact.htm

Landman, J. (2002). Forensic Computing: An Introduction to the Principles and Practical applications. Retrieved from The Electronic Evidence Information Centre http://www.e-evidence.info/biblio.html

McKemmish, R. (1999). What is Forensic Computing? Australian Institute of Criminology: trends & issues in crime and criminal justice. Retrieved from http://www.aic.gov.au/publications/current%20series/tandi/101-120/tandi118.aspx

Nelson, B., Phillips, A., & Steuart, C. (2010). Guide to Computer Forensics and Investigations (4/e). Boston, MA. Course Technology

Newman, R. C. (2007). Policies, Standards, Laws, and Legal Process. In Computer Forensics: Evidence Collection and Management (pp.19-51). Boca Raton, FL: Auerbach Publications

Slay, J., & Koronios, A. (2006). The Australian ethical, legal and standards framework. In Information technology security & risk management (pp. 67-100). Milton, QLD: Wiley

Volonino, L., Anzaldua, R., and Godwin, J. (2007). E-Mail and Webmail Forensics. In Computer Forensics: Principles and Practices (pp. 288-307). Upper Saddle River, NJ. Pearson Prentice Hall

Volonino, L., Anzaldua, R., and Godwin, J. (2007). Fraud and Forensic Accounting Investigation. In Computer Forensics: Principles and Practices (pp. 372-398). Upper Saddle River, NJ. Pearson Prentice Hall

Wright, C. (2009). Law, Investigation, Forensics and Ethics. In Official (ISC)^2 Guide to the CISSP(R)-ISSMP(R) CBK (ISC)2 Press, 1/e. Boston, MA. Auerbach Publications