Communications of the Association for Information Systems

Volume 18 Article 10

9-18-2006

Crime Investigation: A Course in Computer Forensics

Nena Lim
University of Melbourne, nenalim@yahoo.com

Communications of the Association for Information Systems

CRIME INVESTIGATION: A COURSE IN COMPUTER FORENSICS

Nena Lim
Department of Accounting and Business Information Systems
University of Melbourne
limn@unimelb.edu.au

ABSTRACT

The growing amount of crime, such as corporate frauds and virus attacks, in the last two decades highlights not only the importance of computer forensics in crime investigations but also the lack of forensic specialists in this area. An urgent need exists for universities to provide courses on computer forensics to ease the shortage of forensic specialists. This paper proposes a six-dimensional knowledge model for computer forensic courses. The six dimensions include categories of crime, computer technology, security, legislation, investigation process, and forensic tools. The paper describes in detail how the model was implemented in a postgraduate introductory computer forensic course. A brief summary of the lessons learned by the author in the course development and delivery is also presented.

Keywords: Computer forensics, course development

I. INTRODUCTION

The collapse of major corporations in the last decade, such as Enron and WorldCom, shocked the world. To understand what happened and who was responsible for the corporate frauds, investigators employed computer forensics and recovered numerous deleted e-mails and other documents from computers used by the involved parties [Anatasi, 2003]. The rising importance of computer forensics in crime investigations is unsurprising in light of the increasing usage of computers in the last several decades. Governments worldwide emphasize the importance of computer forensics in national security after the September 11, 2001 attack in the United States and London, England bomb attacks [BBC, 2005]. More organizations require computer forensic specialists to conduct non-criminal internal investigations because of employee misbehaviors or intrusions to organizations' computer systems [Sinangin, 2002; Wang et al., 2005].

As computers now play an important role in both computer crime and computer-related crime[1], computer forensic specialists are in demand. More jobs in this area are available in Australia and overseas [ASIO, 2005, ASCLD, 2005]. While the demand for computer forensic specialists

[1] The use of computers as storage devices and communication tools, such as in corporate frauds, is called computer-related crime. In computer crime, such as denial of service attacks and virus attacks, computers become the targets of crime.

increases, the current supply of such professionals is insufficient [Vacca, 2005]. Hence, a need exists for universities to provide courses to ease the shortage of forensic specialists.

In view of the need for universities to train computer forensic specialists, the objective of this paper is to introduce a six-dimensional knowledge model that serves as a framework for any course development in computer forensics. It then summarizes the author's experience of developing a computer forensic course that implemented the knowledge model. The remainder of this paper is organized as follows: Section II explains computer forensics and describes a six-dimensional knowledge model for computer forensic courses. Section III provides the background of a postgraduate computer forensic course that implemented the proposed knowledge model. Section IV presents the course design. It elaborates the topics covered in and the assessment criteria of the course. Section V summarizes the author's experience and provides recommendations to academics who intend to teach similar courses. Finally, Section VI concludes the paper and discusses how a computer forensic course can complement a business forensic course to suit the needs of forensic accountants.

II. COMPUTER FORENSICS

Computer forensics is an "investigation of situations where there is computer-based (digital) or electronic evidence of a crime or suspicious behavior, but the crime or behavior may be of any type" [Mohay et al., 2003, p.3]. It is also "the process of identifying, preserving, analysing, and presenting digital evidence in a manner that is legally acceptable" [McKemmish, 1999]. The above two definitions highlight three important aspects of computer forensics: crime behavior, computer-based evidence, and potential use of evidence in court. A course on computer forensics should provide students the opportunity to learn forensic collection guidelines, laws of evidence, and basic tools used in the forensic examination of computers [Mendell, 2004].

Computer forensics is part of traditional forensic science as well as information systems (IS) security. Table 1 highlights the differences among the disciplines. While more universities offer programs on forensic science [ABC, 2005a] or courses on IS security, to date only limited tertiary institutions offer programs on pure computer forensics. Based on the various definitions of computer forensics, the author proposes that every computer forensic course should cover six dimensions of knowledge as shown in Figure 1.

Six dimensions of computer forensic knowledge:

- Categories of crime: Investigators need to understand how computers are being used in different types of computer crime and computer-related crime.
- Computer technology: Investigators need to know how data are stored in computers so that they know where to search for evidence.
- Security: Investigators need to know how security measures, such as encryption, can protect individuals/organizations as well as hinder investigations.
- Legislation: Investigators should always assume the investigation would go to criminal proceedings. Hence they should be aware of the legislative requirements.
- Investigation process: Investigators must be fully aware of the appropriate procedures of handling evidence so that they do not run the risk of contaminating evidence during the investigation process.
- Forensic tools: Investigators need to know what tools are available for forensic investigations. They also should be aware of the strengths and limitations of each tool.

Table 1. Discipline Characteristics

Discipline	**Characteristics**
Forensic science	Application of a field of science such as biology, chemistry, botany, dentistry, and medicine in order to identify, preserve, analyze, and present evidence in a manner that is legally acceptable. The emphasis is on *physical* evidence, such as fingerprints, blood stain, and DNA.
Information systems security	Protection of information systems against unauthorized access and modification of information. It includes measures that can be used to detect, document, and counter such threats [OrangeSec, 2000].
Computer forensics	The process of identifying, preserving, analyzing, and presenting *digital* evidence in a manner that is legally acceptable [McKemmish, 1999].
Business forensics	Investigation of fraud. It includes quantification of losses/damages arising from a commercial dispute.

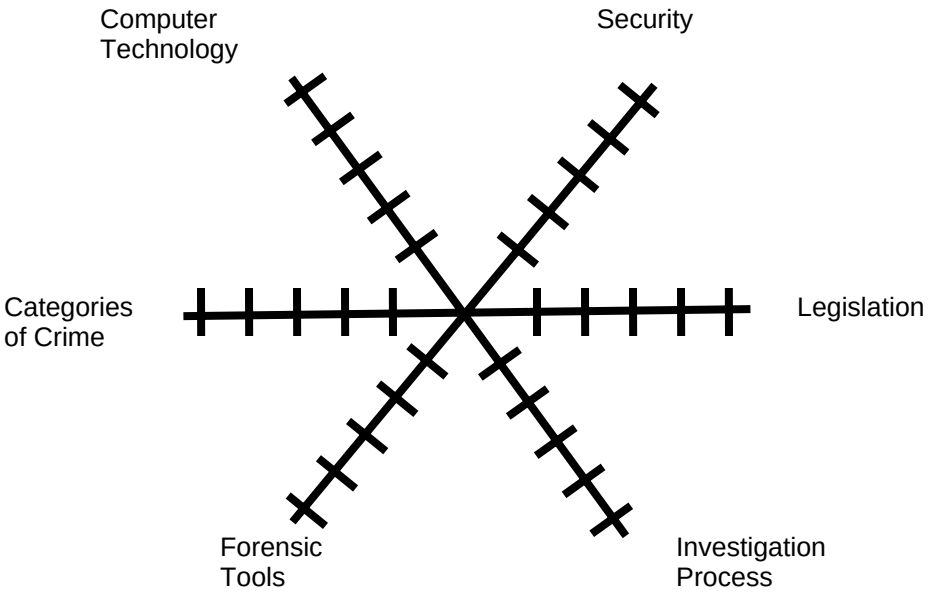

Figure 1. The Six Dimensions of a Computer Forensic Course

III. COURSE BACKGROUND

The proposed knowledge model was implemented in a 12-week postgraduate computer forensic course (course code 306-691). The course is part of a Postgraduate Certificate in Business Forensics offered in the Department of Accounting and Business Information Systems at the University of Melbourne (UM). The postgraduate certificate is a four-course program. Table 2 gives a brief description of the three core courses. Students can take any course as the elective,

but they are recommended to select courses from the psychology or criminology department. The entry requirement for certification is an undergraduate degree and one-year of work experience. As the program is offered on a part-time basis, students are expected to complete it in one year. Students enrolled in other postgraduate programs such as Master of Business and IT (MBIT) and Master of Accounting (MA) can also take the course as an elective.

This course has no prerequisite, but students are expected to have a basic understanding of computer hardware and software at a level equivalent to an introductory course in information systems. Students without the background knowledge are requested to read a chapter on hardware and software in an introductory information systems textbook [Laudon and Laudon, 2005 Chapter 6].

The three-hour seminar course was offered for the first time in July 2005. Twenty-four students enrolled and two audited the course. Among them, 12 students were female and 14 were male. Eleven students were studying for a Master degree in Accounting. Eight students were completing a Master degree in Business & IT. Five were students of the Postgraduate Certificate in Business Forensics. The remaining two were Bachelor of Commerce (Honours) students.

Table 2. Postgraduate Certificate in Business Forensics

Core Course	**Course Coverage**
Forensic Business Processes (306-690)	Identification and collection of accounting and business evidence in fraud investigation; the law of evidence; how to be an expert witness in courts
Accounting Information and Security Valuation (306-667)	Valuation of stock value of entities using the residual income valuation model, discounted cash flow valuation methods, economic value added (EVA); forecasting firms' futures, including risk analysis
Information Technology Forensics (306-691)	Overview of the fundamental concepts related to computer forensics with an emphasis on the overall investigation process

IV. COURSE DESIGN

The objective of the course is to give students an overview of the fundamental concepts related to computer forensics with an emphasis on the overall investigation process. Although many investigation process models were proposed by researchers [e.g., Beebe and Clark, 2005], those models are similar to one another. As discussed in Section II, a computer forensic investigation process generally comprises the identifying, preserving, analyzing, and presenting of digital evidence that is admissible in judicial proceedings. The author developed the course based on the investigation process.

Figure 2 shows the structure and topics of the course. It describes how different topics fit together, in particular how later topics built on the earlier ones. At the beginning of the course, students were introduced to the concept of computer forensics and digital evidence. To understand the important role computers play in cybercrime, students were also introduced to different types of computer crime and computer-related crime. Prior to learning how to conduct a computer forensic investigation, students learned basic knowledge about computers and the Internet. Having laid the foundation, the author then provided an overview of each of the major steps in a computer forensic investigation, which would be elaborated on in later seminars. As legislation is a major component of computer forensics, two lawyers were invited to present the major computer crime legislation, as well as other legal issues salient to computer forensics. The remaining seminars covered the major steps of computer forensics, from discovery of crime to evidence collection, to evidence analysis, and finally to documentation and presentation of evidence.

This course included case discussions in addition to presentations by the lecturer, students, and guests. Students were expected to read a textbook, several newspaper articles, and several journal articles. The details of each seminar, which include materials covered, assigned reading, activities, and references, are summarized in Table 3 and elaborated below. Useful links related to each topic were also provided to students through WebRaft[2]. Appendix I lists some of those links.

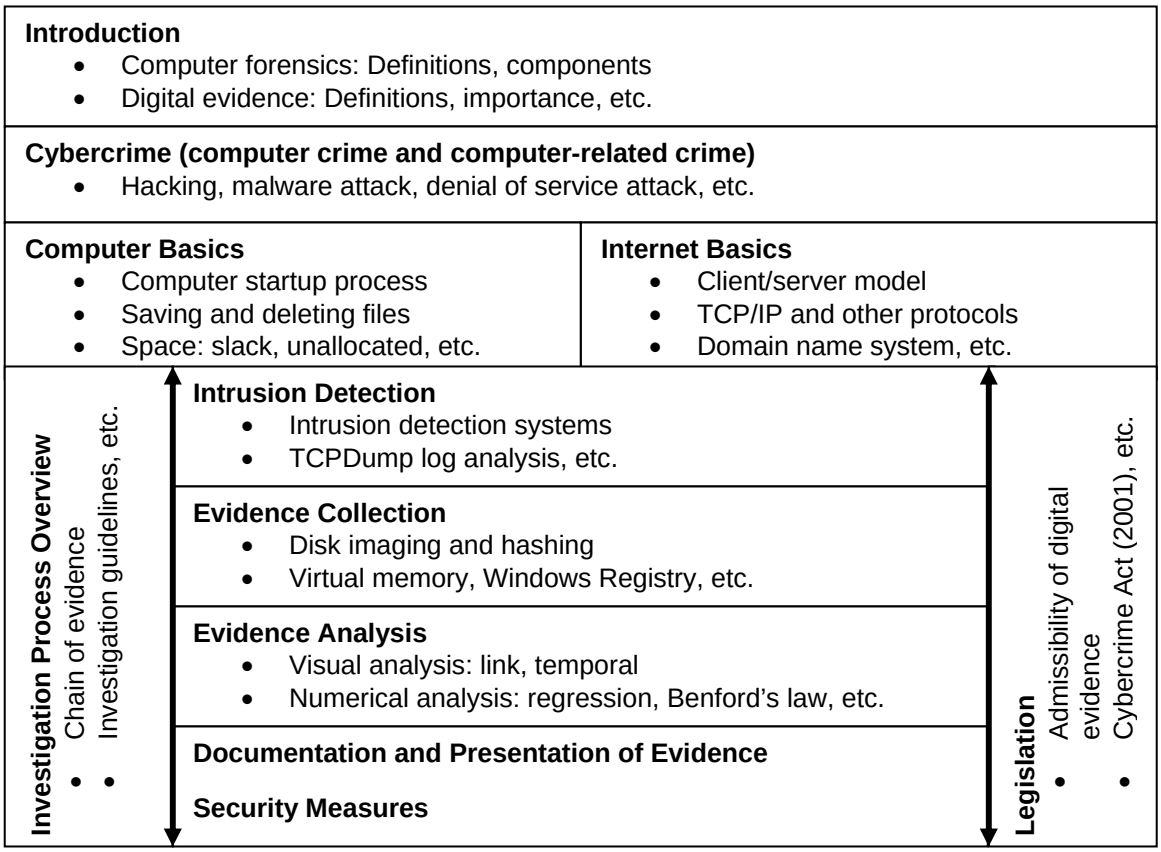

Figure 2. Course Structure and Topics

Table 3. Readings, References, and Activities

Topic	Assigned Readings	Other References	Activities
1. Introduction	Casey [2004] Ch1, Ch2, Ch21.3, Ch22	CSI/FBI Computer Crime and Security Survey 2005, Mohay et al. [2003]	• Discussion of computer crime and computer-related crime. • A glimpse of a video on cyberstalking (the entire video to be shown in Seminar 11)

[2] A proprietary software that is similar to WebCT and Blackboard.

Topic	Assigned Readings	Other References	Activities
			followed by discussion
2. Cybercrime	• Casey [2004] Ch20, Ch21 • Newspaper articles on phishing and pharming: Anonymous [2005a, 2005b] • Articles on spyware: Awad and Fitzgerald [2005], Schmidt and Arnett [2005], Shukla and Nah [2005] • Case on Melissa virus [Mohay, et al., 2003, Ch5.4]	Cole et al. [2005], Peikari and Chuvakin [2004], Wang [2001]	Discussion of Trojan horses
3. Technology Basic	• Casey [2004] Ch8, Ch14, Ch16, Ch17 • Case on keylogging [Mohay, et al., 2003, Ch5.2]	Cole et al. [2005], Nelson et al. [2005]	• Student presentations on spoofing, pharming, spamming • Case discussion: Melissa virus
4. Investigation Process Overview	• Casey [2004] Ch4, Ch6, Ch7, Ch20, Ch23, Ch24 • The Good Practices Guide for Computer Based Electronic Evidence [NHTCU] • Guidelines for the Management of IT evidence [SAI Global, 2003] • Case on misbehaving employee [Mohay, et al., 2003, Ch5.6.1.1]	IACP and USSS [2003], IOCE [2002], Mendell [2004], Mohay et al. [2003], USDJ [2001, 2002]	• Discussion of a crime scene [Nelson et al., 2005, Figure 2-1] • Guest presentation (an expert from KPMG–Dean Newlan) on investigation process • Student presentations on identity theft, software piracy and Internet pornography • Case discussion: keylogging
5. Legislation	• Casey (2004) Ch3 • List of legislation: http://www.aic.gov.au/topics/cybercrime/legal.html	Abraham [2002]	Guest presentation (lawyers from Blake Dawson Waldron–Kellech Smith and Alan Nash) on legislation
6. Intrusion	Casey [2004] Ch19	Deterdeing [2002],	Case discussion:

Topic	Assigned Readings	Other References	Activities
Detection		Middleton [2005], Mohay et al. [2003], Northcut and Novak [2003], Schlarman [2002]	Misbehaving employee
7. Evidence Collection I	• Casey [2004] Ch9, Ch10, Ch23, Ch24 • Article on Windows registry: Carvey [2005a]	Caloyannides [2004], Greenfield [2002], Middleton [2005], Mohay et al. [2003], Schweitzer [2003]	Guest presentation (an expert from KPMG–Peter Moore) on computer forensics including a live demonstration of hard disk imaging
8. Evidence Collection II	Casey [2004] Ch15, Ch18	Greenfield [2002], Nelson et al. [2005], Schweitzer [2003], Stucki [2002]	• Discussion on types of digital evidence • A television program on identity theft [ABC, 2005b]
9. Evidence Analysis I	• Casey [2004] Ch5, Ch9.6 • Case on file signature analysis [Mohay, et al., 2003, Ch5.6.2]	Bhoedjang [2005], Mena [2003], Mohay et al. [2003]	Guest presentation (an expert from Telstra–Roger Levy) on evidence analysis
10. Evidence Analysis II	• Casey [2004] Ch5, Ch9.6 • Articles on Benford's law: Nigrini [1999], Moore and Benjamin [2004]	Chen et al. [2004], Drake and Nigrini [2000], Mena [2003]	• Guest presentation (a colleague in accounting–Matthew Pinnuck) on statistical analysis • Case discussion: File signature analysis
11. Documentation and Presentation of Evidence	Article on evidence presentation [Solon and Harper, 2004]	Cole et al. [2005], Greenstein and Vasarhelyi [2002], MacKey [2003] Ch4, Nelson et al. [2005] Ch14, Oppliger [2003], Schneider [2003]	• Guest presentation (an expert from KPMG–Joel Lucas) on link analysis including a demonstration of a forensic tool, *i2* • The full version of the cyberstalking video followed by discussion.
12. Exam Review and Student Presentation	--	--	Student Presentation of Assignment 3

SEMINAR 1: INTRODUCTION

The author began the course with an introduction to the topic and presented the definitions of computer forensics and digital evidence in Seminar 1. The importance of computer forensics and digital evidence, such as how digital evidence can be used as an alibi, was emphasized. Having highlighted the differences between computer crime and computer-related crime, the author asked students to form into groups and provide examples of each type of crime. In addition, the beginning section of a crime video was shown to generate in-class discussions [RTHK, 2003]. Although titled "Blackmail," the video is about cyberstalking. In the video, a girl receives threatening emails from a cyberstalker who monitors her online activities through a Trojan horse. He also steals her identity in online chat rooms. The story is about how the police investigate the case. They track the cyberstalker through his IP address, narrow down the investigation scope to a handful of employees in a trading company, identify the relevant computers, and crack the password of a file that provides the required evidence to indict an IT manager of the company. Students were shown only the first few minutes of the clip, which shows the girl receiving threatening emails. They then discussed possible investigation approaches to solve the case. They would watch the entire 20-minute video clip at the end of the semester.

SEMINAR 2: CYBERCRIME

Seminar 2 introduced students to different concepts related to cybercrime. Topics covered included hacking, viruses, worms, Trojan horses, spyware, keylogger attack, denial of service attacks, and phishing. To facilitate the understanding of how cybercrime is committed, the author explained basic computer and network knowledge along the way. For example, packet switching, Transmission Control Protocol/Internet Protocol (TCP/IP), IP address, domain name system (DNS), and client/server model were covered. During the seminar, students discussed different aspects of Trojan horses such as who is likely to spread Trojan horses.

At the end of the class, students were asked to read two newspaper articles at home, which discuss phishing and pharming [Anonymous, 2005a; 2005b]. They were also asked to read a case on the Melissa virus attack in 1999 [Mohay et al., 2003] for the following week's discussion. *The Communications of the ACM* published a special issue on spyware in August 2005. Three of the articles in that issue [Awad and Fitzgerald, 2005; Schmidt and Arnett, 2005; Shukla and Nah, 2005] were included in the assigned reading later in the semester. The author selected those three articles because they were short, interesting, and easy to read.

SEMINAR 3: TECHNOLOGY BASIC

Seminar 3 continued to cover basic computer and network knowledge essential to the understanding of collecting digital evidence. The author explained the computer start-up process and its significance in computer forensics. Other topics covered in this class included hard disk structure, CHS (cylinder, head, and sector) addressing, file systems, allocated space, unallocated space, slack space, file signature, and MAC (media access control) address. Moreover, the students engaged in a group discussion on the Melissa virus case that was distributed the week before [Mohay et al., 2003]. They were given another case on keylogging for the following week's discussion [Mohay et al., 2003].

To enhance students' involvement in the course, the author deliberately left out six cybercrime related topics from her presentation in the seminars. Students formed into groups to investigate those topics and presented the results to the class. Each group had 15 minutes to do their presentation. The six arbitrarily selected topics were spamming, spoofing, pharming, identity theft, software piracy, and Internet pornography. In Seminar 3, students presented spamming, spoofing, and pharming.

SEMINAR 4: INVESTIGATION PROCESS OVERVIEW

Through the discussion of a crime scene [Nelson et al., 2005, Figure 2-1], the author provided an overview of the entire process of a cybercrime investigation in Seminar 4. Criminology concepts such as the Locard's exchange principle[3] and modus operandi[4] were explained. In particular, she explained the importance for investigators to "show that the evidence remained uncontaminated after it was gathered and during analysis" [Mohay et al., 2003, p.27]. This is called the *chain of evidence* principle. The author briefly described how this principle should be maintained during the investigation process. The details of how the principle should be upheld in each investigation step would be covered in later seminars. Students were required to read *The Good Practice Guide for Computer Based Electronic Evidence* developed by the National Hi-Tech Crime Unit [NHTCU] and the *Guidelines for the Management of IT Evidence* [SAI Global, 2003]. They were also given a case on chain of evidence for discussions in Seminar 6 [Mohay et al., 2003]. Mr. Dean Newlan, Executive Director of KPMG Forensic, gave a presentation on how he and his colleagues conduct computer forensic investigations. In addition, the other half of the students gave their presentation on software piracy, identity theft, and Internet pornography. Students also participated in a discussion of a case in which the FBI used a keylogger to steal an organized gang leader's password [Mohay et al., 2003].

SEMINAR 5: LEGISLATION

Seminar 5 focused on Australian legislation on computer crime and computer-related crime. The seminar was run by two Supreme Court lawyers, Ms. Kellech Smith and Mr. Alan Nash, who presented various types of computer crime-related legislation, civil courses of actions, admissibility of evidence, and gathering and preservation of evidence. As much legislation is related to computer crime, they focused only on the major ones: CyberCrime Act (2001), Criminal Code Act 1995 (Cth), Evidence Act (1995), Copyright Act 1968 (Cth), Electronic Transactions Act 1999 (Cth), and Spam Act (2003). Moreover, they highlighted the importance of obtaining warrants and/or Anton Piller Orders (i.e., civil search warrants) in the evidence collection process.

SEMINAR 6: INTRUSION DETECTION

Half of the course (Seminar 6 to Seminar 11) elaborated on each step in the computer forensic investigation process. It began with Seminar 6 that covered discovery of crime in particular intrusion detection. In addition to different phases of intrusion, different approaches of intrusion, different categories of intrusion detection system, students learned how to monitor Windows systems and network systems. They were introduced to the network monitoring tools *netstat*, *nmap*, and *fport*. The author also taught the students how to interpret simple network activities reports generated by *tcpdump*. *Tcpdump* is a network monitoring tool for identifying abnormal network activities such as hacking or denial of service attack [Northcutt and Novak, 2003]. The author also explained how someone can trigger a denial of service attack using TCP/IP or Internet Control Message Protocol (ICMP). Furthermore, a case related to chain of evidence (misbehaving employee) was discussed in class [Mohay et al., 2003].

SEMINARS 7 AND 8: EVIDENCE COLLECTION

Both seminars 7 and 8 were about identification and seizure of evidence. Seminar 7 focused on collecting digital evidence from a stand-alone computer. It covered disk imaging, hashing, collecting evidence stored in virtual memory, printer spooler files, hidden files, and Windows

[3] The Locard's exchange principle states that "anyone, or anything, entering a crime scene takes something of a scene with them, and leaves something of themselves behind when they leave" [Casey, 2004 p. 96].

[4] Modus operandi refers to "the behaviors that are committed by a criminal for the purpose of successfully completing an offense" [Casey, 2004, p. 149].

registry. A KPMG forensic expert, Mr. Peter Moore, presented how he conducted computer forensic investigations. He also demonstrated how to image a hard drive using Encase, the de facto industrial standard, to collect evidence from a computer. Seminar 8 focused on collecting digital evidence from a networked computer environment, such as Web browsers and e-mails. Apart from discussing different types of digital evidence, students were shown part of a television program on identity theft [ABC, 2005b].

SEMINARS 9 AND 10: EVIDENCE ANALYSIS

Seminars 9 and 10 concerned evidence analysis. Seminar 9 covered how data mining techniques could be used to identify useful evidence. It also covered different evidence analysis approaches: system usage, Internet usage, temporal, link, function, classification, association, sequential, clustering, deviation detection, and string comparison. A senior manager from the largest telecommunication company in Australia, Telstra, Mr. Roger Levy, explained how his colleagues employed data mining to investigate crime. Students were given a case on file signature analysis for the following week's discussion [Mohay et al., 2003].

In Seminar 10, a colleague in accounting, Associate Professor Matthew Pinnuck, gave a presentation on statistical analysis. He presented regression analysis, correlation analysis, and dispersion analysis. The author also introduced Benford's law [Nigrini, 1999; Moore and Benjamin, 2004] to the class and illustrated how it could be used in evidence analysis. In addition, a case related to file signature analysis was discussed.

SEMINAR 11: DOCUMENTATION AND PRESENTATION OF EVIDENCE

At the beginning of Seminar 11, Mr. Joel Lucas, another KPMG forensic expert, demonstrated how to use a link analysis software called *i2* to analyze digital evidence. In addition to documentation and presentation of evidence in court [Solon and Harper, 2004], Seminar 11 covered computer and Internet security. In particular, the author explained the concept of private key and public key encryptions and how encryption could protect individuals/organizations as well as hinder investigation. The entire video of the cyberstalking case was also shown, followed by a class discussion. The video summarized the steps in a computer forensic investigation and the topics covered in this course.

SEMINAR 12: EXAMINATION REVIEW AND PRESENTATION

The last seminar was a review of materials covered in the semester. In addition, students presented the newspaper articles they wrote for Assignment 3.

ASSESSMENT SCHEME

Table 4 shows the assessment scheme of the course. As explained earlier, students did a group presentation on a topic related to computer crime (spamming, pharming, spoofing, software piracy, identity theft, and Internet pornography) in either Seminar 3 or 4. The presentation was worth 10 percent of their final grade. Another 10 percent was based on class participation. Students were required to submit three assignments. The first two assignments were individual assignments, each worth 5 percent. Assignment 1 (Appendix II) concerned how files were saved and deleted on a hard drive. It tested students' understanding of concepts on allocated space, unallocated space, and slack space. Assignment 2 (Appendix III) was about network intrusion detection. It tested students' ability to interpret network activities reports to identify abnormal network activities. Assignment 3 (Appendix IV) was worth 20 percent. Students were required to form into groups and write a newspaper-style article on a topic related to the course. They were also required to present their work in the last seminar. The topics selected by students for assignment 3 were as follows:

- Wireless network security

- Biometrics
- Forensic accounting
- Music piracy
- Mobile phones and personal digital assistants (PDAs) forensics
- Romance scams
- Prevention of computer crime
- Employee monitoring

Students took a two-hour, closed-book final examination at the end of the semester. The final examination accounted for 50 percent of their total grade.

Table 4. Assessment Scheme

Group Presentation	10%
Class Participation	10%
Assignment 1 (on file space)	5%
Assignment 2 (on network intrusion)	5%
Assignment 3 (writing a newspaper article plus presentation)	20%
Final Examination	50%
Total	100%

V. LESSONS LEARNED AND RECOMMENDATIONS

Results of an end-of-semester anonymous survey showed that most students found the course interesting and useful. This section summarizes the author's experience of developing and teaching the computer forensics course, and her recommendations for academics who would like to develop a similar course.

First, the extent of coverage of the above computer forensic course in terms of the six dimensions is shown in Figure 3. The course successfully covered all six dimensions of the proposed knowledge model to different degrees. In particular, it emphasized the computer forensic investigation process. Feedback from the students indicated that the strength of the course lay in the breadth of the course. The above implementation is suitable for courses of 10 to 12 weeks' duration. For 15-week courses, academics may consider increasing coverage of technology and security. For example, they could extend the coverage of the computer technology dimension to include a more detailed discussion of computer file systems specific to each major operating system in the market. If resources are available, academics may consider giving students hands-on practice of forensic tools in a laboratory so that students can practice imaging a hard disk or recovering deleted files. For an advanced computer forensic course, academics may consider teaching password recovery techniques or PDAs recovery techniques [Jansen and Ayers, 2004].

Second, while it is generally a good idea to invite practitioners to an IS course to share their experience, an active involvement of practitioners is a must for the success of a computer

forensic course. This is chiefly because while IS academics are likely to have some working experience in information systems, they are unlikely to have much experience in computer forensics. Without the involvement of practitioners, students probably would consider the course to be too theoretical. Comments from the students of the computer forensic course confirmed this thought. One third of the students of course 306-691 considered the guest presentations the biggest strength of the course. In particular, they valued the demonstration of different forensic tools by the guest speakers. Among all the guest speakers in 306-691, students most liked the presentation by the senior manager from Telstra.

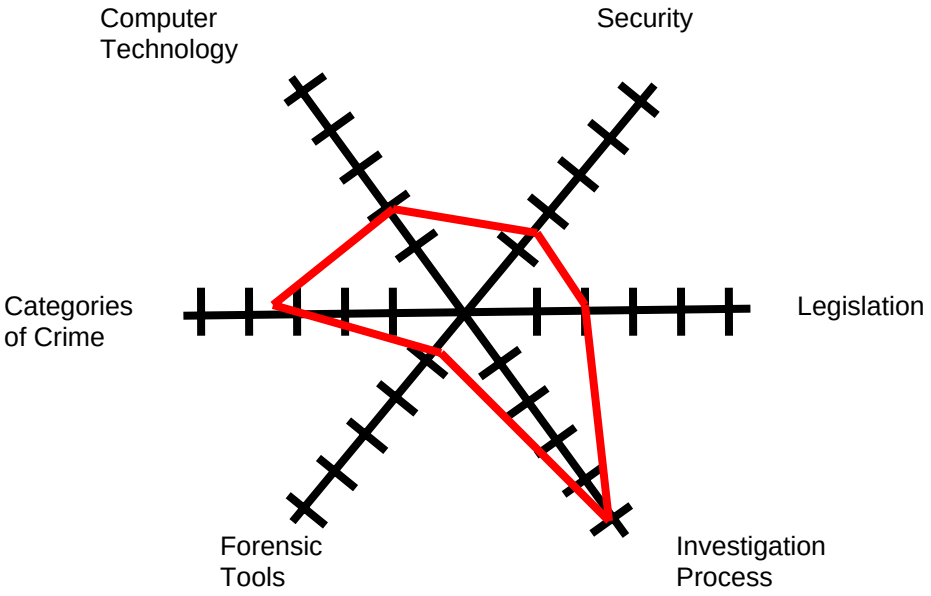

Figure 3. Implementation of the Six Dimensions

The involvement of multiple guest speakers requires academics to be flexible and ready to fit the course into the busy schedule of the practitioners. On more than one occasion the author experienced that guests were unable to present to the class as scheduled. For example, the two lawyers who presented in Seminar 4 were, in fact, a replacement for another more experienced lawyer who became unavailable suddenly because of an impending court case. Therefore, it is important to have a contingency plan, such as preparing extra material related to each topic should the scheduled guests be unavailable.

Third, developing a computer forensic course is not just another new course development for IS academics. Academics are unlikely to have much background knowledge in computer forensics, except in computer technology and security. Therefore, the amount of time and effort required to develop such a course, including the time required to learn the materials, is immense. The author would not recommend any academic who plans to develop a similar course to do it alone. Departmental support, for example, by providing sufficient resources such as reduced teaching loads for course preparation or funding for purchasing forensic software[5], is vital. The time constraint faced by the author was reflected in the last assignment. Because of the practical

[5] Each copy of Encase Version 5 costs about $4000.

nature of the course, it would be a good idea to let students illustrate their understanding by solving a case. Unfortunately, as the author did not have enough time to finish writing a case for that purpose, she was forced to give up the idea and required the students to write a newspaper article instead.

Fourth, selecting an appropriate textbook for a computer forensic course can be a challenge. While many IS security textbooks are available in the market, textbooks for computer forensics, in particular from traditional publishers, are limited. The existing forensic books can be classified into three categories:

- Books that focus on general concepts on computer forensics [e.g., Mohay et al., 2003; Vacca, 2005].
- Books that focus on technical details of computer forensics such as where to locate log files [e.g., Carvey, 2005b; Nelson et al., 2005].
- Books that cover both general concepts and technical details of computer forensics [e.g., Casey, 2004; Mandia et al., 2003].

The author chose Casey [2004] as the textbook because it has a reasonable balance of general concepts and technical details. Nevertheless, two problems existed. First, although Casey [2004] covers computer crime legislation, it is inappropriate for Australian students as it is about American legislation. Second, it appears that the book was not written for students. Therefore, some students were dissatisfied with the book as it does not have features such as end-of-chapter exercises, which they normally found in other well-developed textbooks. Some students also found the book content too technical. Despite these problems, the author still considers Casey [2004] to be the best choice in the market at the moment. Apart from books, academics are recommended to search for information on computer forensics from the following three journals: *Digital Investigation*, *International Journal of Digital Evidence*, and *Journal of Digital Forensics, Security and Law* (a new journal that starts in 2006).

VI. CONCLUSION

In this paper, the author proposed a six-dimensional knowledge model for computer forensic courses. She also described how she implemented the model in a trial run of a postgraduate computer forensic course in 2005. As the course is only an introductory course in computer forensics, the author does not expect students to become certified examiners after taking the course. Nevertheless, the materials covered in the course should provide the students with a good starting point if they intend to pursue a career in this area. Students can consider the CIFI (Certified Information Forensics Investigator) certification of the IISFA (International Information Systems Forensics Association) or the CCE (Certified Computer Examiner) certification of the ISFCE (International Society of Forensic Computer Examiners).

Apart from training students to become certified computer forensic specialists, IS academics may consider collaborating with accounting colleagues to develop a curriculum that combines business forensics and computer forensics. Business forensics is mainly about fraud investigation. In a business forensic course, students learn about fraud investigation, quantification of losses/damages arising from a commercial dispute, law of evidence, and how to be an expert witness in courts. Equipped with knowledge from both business forensics and computer forensics, students would be ready to work as forensic accountants in accounting practices such as the Big Four Firms.

ACKNOWLEDGMENTS

The author thanks Peter Seddon, Annisa Tong, Iris Vessey and the associate editor for their helpful comments.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that
1. these links existed as of the date of publication but are not guaranteed to be working thereafter.
2. the contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. the author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. the author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

ABC. (2005a) *Want to Be a Forensic Investigator/Scientist?* http://www.abc.net.au/science/forensic/wannabe.htm (current Jan. 4, 2006).

ABC. (2005b) "Your Money & Your Life", *Four Corners (TV Program)*, Aug. 15, http://www.lib.unimelb.edu.au/collections/media/vidi_str.html#mc_v178 (current Mar. 31, 2006).

Abraham, A. (2002) "Chapter 7: Cyber Forensics and the Legal System" in Marcella, A. J. and R. S. Greenfield (eds.) *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, Boca Raton, Florida: Auerbach Publications, pp. 133-146.

Anastasi, J. (2003) *The New Forensics: Investigating Corporate Fraud and the Theft of Intellectual Property*, Hoboken, New Jersey: John Wiley & Sons, Inc.

Anonymous (2005a) "Phishers Take up Pharming", *The Australian IT Business*, May 17, p. 2.

Anonymous (2005b) "Hero Hackers May Make Things Worse", *The Australian IT Business*, May 31, p. 4.

ASCLD (American Society of Crime Laboratory Directors) (2005) *Employment Opportunities*, http://www.ascld.org/employment.html (current Oct. 14, 2005).

ASIO (Australian Security Intelligence Organisation) (2005) *Employment: Computer Forensic Specialist*, http://www.asio.gov.au/Employment/Content/Vacancies/computer_forensic_specialist.html (current Oct. 14, 2005).

Awad, N. F. and K. Fitzgerald (2005) "The Deceptive Behaviors That Offend US Most about Spyware", *Communications of the ACM*, 48(8), pp. 55-60.

BBC. (2005) "Tracking a Suspect by Mobile Phone", *BBC News*, Aug. 3, 2005, http://news.bbc.co.uk/1/hi/technology/4738219.stm (current Jan. 20, 2006).

Beebe, N. L. and J. G. Clark (2005) "A Hierarchical, Objective-Based Framework for the Digital Investigation Process", *Journal of Digital Investigation*, 2(3), pp. 147-167.

Bhoedjang, R. A. F. (2005) "Robust Disk Imaging with RDD and MIDAS" presented by Z. Geradts at the Computer Forensics Workshop, *17th Meeting of the International Association of Forensic Sciences*, Hong Kong.

Caloyannides, M. A. (2004) *Privacy Protection and Computer Forensics*, *2nd edition*, Norwood, MA: Artech House.

Carvey, H. (2005a) "The Windows Registry as a Forensic Resource", *Digital Investigation*, 2(3), pp. 201-205.

Carvey, H. (2005b) *Windows Forensics and Incident Recovery*, Boston, MA: Addison Wesley.

Casey, E. (2004) *Digital Evidence and Computer Crime: Computer Science, Computers and the Internet*, *2nd edition*, London, UK: Elsevier Academic Press.

Chen, H. et al. (2004) "Crime Data Mining: A General Framework and Some Examples", *IEEE Computer*, 37(4), pp. 50-56.

Chisum, W. J. and B. E. Turvey (2000) "Evidence Dynamics: Locard's Exchange Principle & Crime Reconstruction", *Journal of Behavorial Profiling*, (1)1, pp. 1-9.

Cole, E., R. Krutz, and J. W. Conley (2005) *Network Security Bible*, Indianapolis, Indiana: Wiley Publishing, Inc.

Deterdeing, B. (2002) "Chapter 5: Tools of the Trade: Automated Tools Used to Secure a System Throughout the Stages of a Forensic Investigation" in Marcella, A. J. and R. S. Greenfield (eds.) *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, Boca Raton, Florida: Auerbach Publications, pp. 97-116.

Drake, P. D. and M. J. Nigrini (2000) "Computer Assisted Analytical Procedures Using Benford's Law", *Journal of Accounting Education*, 18(2), pp. 127-146.

Gladyshev, P. (2005) "Finite State Machine Analysis of a Blackmail Investigation", *International Journal of Digital Evidence*, 4(1), pp. 1-13.

Greenfield, R. E. (2002) "Chapter 3: The Liturgical Forensic Examination: Tracing Activity on a Windows-Based Desktop" in Marcella, A. J. and R. S. Greenfield (eds.) *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, Boca Raton, Florida: Auerbach Publications, pp. 47-77.

Greenstein, M. and M. Vasarhelyi (2002) *Electronic Commerce: Security, Risk Management, and Control*, New York, NY: McGraw-Hill Irwin.

IACP (International Association of Chiefs of Police) and USSS (United States Secret Service) (2003) *Best Practices for Seizing Electronic Evidence*, http://www.secretservice.gov/electronic_evidence.shtml, (current Apr. 15, 2006).

IOCE (International Organization on Computer Evidence) (2002) *Guidelines for Best Practice in the Forensic Examination of Digital Technology*, V1.0, http://www.ioce.org/2002/Guidelines%20for%20Best%20Practices%20in%20Examination%20of%20Digital%20Evid.pdf (current Apr. 15, 2006).

Jansen, W. and R. Ayers (2004) *Guidelines on PDA Forensics: Recommendations of the National Institute of Standards and Technology*, Serial Number 800-72, National Institute of Standards and Technology, pp. 1-59.

Laudon, K. C. and J. P. Laudon (2005) *Essentials of Management Information Systems, 6th edition*, Upper Saddle River, New Jersey: Pearson Education Inc.

MacKey, D. (2003) *Web Security For Network and System Administrators*, Boston, Massachusetts: Thomson Course Technology.

Mandia, K., C. Prosise, and M. Pepe (2003) *Incident Response & Computer Forensics, 2nd edition*, New York, NY: McGraw-Hill, Osborne.

McKemmish, R. (1999) "No. 118 What is Forensic Computing?" *Australian Institute of Criminology Trends and Issues in Crime and Criminal Justice* http://www.aic.gov.au/publications/tandi/ti118.pdf (current Apr. 1, 2006).

Mena, J. (2003) *Investigative Data Mining for Security and Criminal Detection*, Boston, MA: Butterworth Heinemann, Elsevier Science.

Mendell, R. (2004) *Investigating Computer Crime in the 21st Century*, *2nd edition,* Springfield, Illinois: Charles C. Thomas Publisher, Ltd.

Middleton, B. (2005) *Cyber Crime Investigator's Field Guide*, *2nd edition*, Boca Raton, Florida: Auerbach Publications.

Mohay, G. et al. (2003) *Computer and Intrusion Forensics*, Norwood, MA: Artech House.

Moore, G. B. and C. O. Benjamin (2004) "Using Benford's Law for Fraud Detection", *Internal Auditing*, 19(1), pp. 4-9.

Nelson, B. et al. (2005) *Guide to Computer Forensics and Investigations*, *2nd edition*, Boston, Massachusetts: Thomson Course Technology.

NHTCU (National Hi-Tech Crime Unit) (?) *Good Practice Guide for Computer Based Electronic Evidence*, pp. 1-51, http://www.nhtcu.org/media/documents/publications/ACPO_Guide_for_computer-based_electronic_evidece.pdf (current Mar. 31, 2006).

Nigrini, M. J. (1999) "I've Got Your Number", *Journal of Accountancy*, 187(5), pp. 79-83.

Northcutt, S. and J. Novak (2003) *Network Intrusion Detection*, *3rd edition,* Indianapolis, Indiana: New Riders Publishing.

Oppliger, R. (2003) *Security Technologies for the World Wide Web*, *2nd edition,* Norwood, MA: Artech House.

OrangeSec (2000) *Definitions – Information Systems Security*, http://www.orangesec.com/definitions.html (current Jul. 11, 2006).

Peikari, C. and A. Chuvakin (2004) *Security Warrior*, Sebastopol, CA: O'Reilly.

RTHK (Radio Television Hong Kong) (2003) "Blackmail," *Justice Through Science: Episode 10*, http://www.iafs2005.com/eng/hkforensicprog.php#10 (current Aug. 26, 2005).

SAI (Standards Australia International) Global (2003) *Guidelines for the Management of IT Evidence*, HB171-2003.

Schlarman, S. (2002) "Chapter 6: Network Intrusion Management and Profiling" in Marcella, A. J. and R. S. Greenfield (eds.) *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, Boca Raton, Florida: Auerbach Publications, pp. 117-132.

Schmidt, M. B. and K. P. Arnett (2005) "Spyware: A Little Knowledge is a Wonderful Thing", *Communications of the ACM*, 48(8), pp. 67-70.

Schneider, G. P. (2003) "Chapter 11: Implementing Electronic Commerce Security," *Electronic Commerce*, *4th Edition*, Boston, MA: Thomson Course Technology, pp. 445-484.

Schweitzer, D. (2003) *Incident Response*, Indianapolis, Indiana: Wiley Publishing Inc.

Shukla, S. and F. F. Nah (2005) "Web Browsing and Spyware Intrusion," *Communications of the ACM*, 48(8), pp. 85-90.

Sinangin, D. (2002) "Computer Forensics Investigations in a Corporate Environment", *Computer Fraud & Security*, (2002)6, pp.11-14.

Solon, M. and P. Harper (2004) "Preparing Evidence for Court", *Digital Investigation*, 1(4), pp. 279-283.

Stucki, C. (2002) "Chapter 2: How to Begin a Non-Liturgical Forensic Examination" in Marcella, A. J. and R. S. Greenfield (eds.) *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, Boca Raton, Florida: Auerbach Publications, pp. 19-45.

USDJ (United States Department of Justice) (2001) *Electronic Crime Scene Investigation: A Guide for First Responders*, Technical Working Group for Electronic Crime Scene Investigation, http://www.ncjrs.gov/pdffiles1/nij/187736.pdf (current Apr. 15, 2006).

USDJ (United States Department of Justice) (2002) *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Computer Crime and Intellectual Property Section, Criminal Division, http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm (current Apr. 15, 2006).

Vacca, J. R. (2005) *Computer Forensics: Computer Crime Scene Investigation, 2nd edition*, Hingham, Massachusetts: Charles River Media, Inc.

Wang, W. (2001) *Steal This Computer Book 2: What They Don't Tell You About the Internet*, San Francisco CA: No Starch Press.

Wang, Y., J. Cannady, and J. Rosenbluth (2005) "Foundations of Computer Forensics: A Technology for the Fight Against Computer Crime", *Computer Law & Security Report*, (21)2, pp.119-127.

BIBLIOGRAPHY

Caloyannides, M. A. (2002) *Desktop Witness: The Do's and Don'ts of Personal Computer Security*, West Sussex, England: John Wiley & Sons, Ltd.

Chantico Publishing Company, Inc. (1992) *Combating Computer Crime: Prevention, Detection, Investigation*, New York, NY: McGraw-Hill, Inc.

Clark, F. and K. Diliberto (1996) *Investigating Computer Crime*, Boca Raton, Florida: CRC Press.

Marcella, A. J. and R. S. Greenfield (eds.) (2002) *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, Boca Raton, Florida: Auerbach Publications.

Matsuura, J. H. (2002) *Security, Rights, and Liabilities in E-Commerce*, Norwood, MA: Artech House.

Moscove, S., M. Simkin, and N. Bagranoff. (2003) "Chapter 11: Computer Crime and Ethics", *Core Concepts of Accounting Information Systems*, *8th edition,* New York, NY: John Wiley & Sons, Inc., pp. 319-350.

Parker, D. B. (1998) *Fighting Computer Crime: A New Framework for Protecting Information*, New York, NY: Wiley Publishing.

Stephenson, P. (2000) *Investigating Computer-Related Crime*, Boca Raton, Florida: CRC Press.

APPENDIX I. USEFUL LINKS

Organizations related to computer crime	**Web Site**
Australia	
• Australian High Tech Crime Centre (AHTCC)	http://www.ahtcc.gov.au/
• Australian Institute of Criminology (AIC)	http://www.aic.gov.au/
• National Institute of Forensic Science	http://www.nifs.com.au/
• Australian Computer Emergency Response Team (AusCERT)	http://www.auscert.org.au/
• Australian Government Information Management Office	http://www.agimo.gov.au/
• Australian Government NetAlert Limited	http://www.netalert.net.au/default.asp
Others	
• National Hi-Tech Crime Unit (NHTCU) – UK	http://www.nhtcu.org/ngcontent.cfm?a_id=12261
• Virtual Global TaskForce	http://www.virtualglobaltaskforce.com/index-corporate.html
• Anti-Phishing Working Group (APWG)	http://www.antiphishing.org/
• International Organization on Computer Evidence	http://www.ioce.org/
Good Practice Guides	
• Good Practice Guide for Computer-Based Electronic Evidence [NHTCU]	http://www.nhtcu.org/media/documents/publications/ACPO_Guide_for_computer-based_electronic_evidece.pdf
• Guidelines for Execution of Search Warrants by Australian Federal Police on Behalf of Australian Government Departments and Agencies	http://www.afp.gov.au/afp/page/GovCorporate/warrants.htm
• Best Practices for Seizing Electronic Evidence [IACP and USSS, 2003]	http://www.secretservice.gov/electronic_evidence.shtml
• Electronic Crime Scene Investigation: A Guide for First Responders (USDJ, 2001)	http://www.ncjrs.gov/pdffiles1/nij/187736.pdf
Readings	

• CSI/FBI Computer Crime and Security Survey 2005	http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf
• "Evidence Dynamics: Locard's Exchange Principle & Crime Reconstruction" [Chisum and Turvey, 2000]	http://www.profiling.org/journal/vol1_no1/jbp_ed_january2000_1-1.html
• High Tech Crime Brief on Computer Crime AIC	http://www.aic.gov.au/publications/htcb/
Journals	
• International Journal of Digital Evidence	http://www.ijde.org/index.html
• Digital Investigation	http://www.digitalinvestigation.net/
Forensic Tools	
• Encase	http://www.guidancesoftware.com/commercial/index.asp
• Forensic Toolkit (FTK)	https://www.accessdata.com/

APPENDIX II. ASSIGNMENT 1

Background Information *Adapted from Gladyshev [2005]*

Sandra Welke is a manager in the marketing department in a company based in Melbourne. On July 10, 2005, she received an anonymous letter. The letter was addressed to her and contains a number of allegations and threats. From the content of the letter, Miss Welke believed that the letter came from one of her colleagues, Tony Bush. She contacted the police immediately and handed them the letter. The Victorian police went to see Mr. Bush and found that he went on holiday abroad the night before. Mr. Bush works in the accounting department. The police seized his computer from his office. They also interviewed Mr. Bush as soon as he returned to Australia. Mr. Bush admitted that he wrote a letter with allegations on his office computer and was going to send the letter to the Managing Director. Yet he said he gave up the idea at the last minute and did not send out the letter. He also denied making any threat. Mr. Bush argued that as Miss Welke had access to his computer while he was on holiday, it was possible that Miss Welke added the threats to the letter to frame him.

The police examined the hard drive of Mr. Bush's computer. They found a total of 15 recognisable fragments of the letter located in various areas of the disk space. One of the fragments was a "clean" letter without threats, stored in an active file. All other fragments contained threats and were found in unallocated disk space or slack space. The timestamps for all fragments were dated before July 9.

One of the letter fragments was found in the slack space of another letter unconnected with the incident. The person to whom the letter was addressed lives in Western Australia. When the police interviewed him, he confirmed that he had received the letter in the morning on the day that Mr. Bush had gone abroad on holiday.

Please answer the following questions based on the above information.

(a) What is unallocated space? How is it different from slack space? What is/are the possible reason(s) that fragments of the letter were found in the unallocated disk space?

(b) Based on the above evidence, do you believe the letter with threats was written after Mr. Bush going on holiday?

APPENDIX III. ASSIGNMENT 2

Please answer the questions relating to the following two scenarios. *Adapted from Northcutt and Novak [2003]*

(a) Calvin is the system administrator of a company based in Melbourne. One of his duties is to monitor network activities. When he returned to his office from holiday on July 18, 2005, he received two tcpdump reports as below. What activities can he conclude from these two reports? What is the difference between these two reports?

July 16, 2005

00:05:54.56000 scanner.net > 192.168.117.129: icmp: echo request

00:06:01.87000 scanner.net > 192.168.117.139: icmp: echo request

00:12:44.77000 scanner.net > 192.168.117.242: icmp: echo request

00:15:39.19000 scanner.net > 192.168.117.63: icmp: echo request

00:15:59.71000 scanner.net > 192.168.117.233: icmp: echo request

00:18:29.79000 scanner.net > 192.168.117.89: icmp: echo request

July 17, 2005

00:51:16.26000 scanner.net > 192.168.117.255: icmp: echo request

00:51:17.30000 scanner.net > 192.168.117.0: icmp: echo request

00:51:18.20000 scanner.net > 192.168.118.255: icmp: echo request

00:51:18.33000 scanner.net > 192.168.118.0: icmp: echo request

00:51:19.23000 scanner.net > 192.168.119.255: icmp: echo request

00:52:05.13000 scanner.net > 192.168.119.0: icmp: echo request

00:52:05.95000 scanner.net > 192.168.120.255: icmp: echo request

00:52:65.53000 scanner.net > 192.168.120.0: icmp: echo request

(b) A local ISP receives a phone call from a user who states that he cannot access the mail server. The ISP technician conducts a review of the mail server and does not see any problems. She believes it is not the host itself creating the problem, but rather some sort of network-based attack. She decides to capture network traffic using tcpdump. Look at the tcpdump output below, what common attack is she faced with? What would you suggest to mitigate such attacks? Note: The ISP technician also finds out that the source IP addresses do not exist.

12:17:45.3215 64.42.33.170.1022 > mail.host.com.110: S 1465873791:1465873791(0) win 4096

12:17:45.4714 64.42.33.171.1022 > mail.host.com.110: S 1465873792:1465873792(0) win 4096

12:17:45.8637 64.42.33.172.1022 > mail.host.com.110: S 1465873793:1465873793(0) win 4096

12:17:45.9719 64.42.33.173.1022 > mail.host.com.110: S 1465873794:1465873794(0) win 4096

12:17:46.1252 64.42.33.174.1022 > mail.host.com.110: S 1465873795:1465873795(0) win 4096

12:17:46.4634 64.42.33.175.1022 > mail.host.com.110: S 1465873796:1465873796(0) win 4096

APPENDIX IV. ASSIGNMENT 3

This assignment is worth 20% of your total marks. Students are expected to form a group of three. Imagine your group works for *The Australian* newspaper. Knowing that your group has taken a course in computer forensics, the Chief Editor of the IT section of *The Australian* asks your group to write a newspaper article on Information Technology Forensics. Apply what you have learned in this course, select a topic of your choice, and write a newspaper article. Here are some topics that you might want to write about, but you can select any topic of your choice.

- IT forensic training in Australia or a country of your choice
- Employee privacy in the workplace and forensic investigation
- Prevention of computer crime
- Digital evidence from mobile telephones and PDAs

Please send me an email to register your topic. You are expected to submit a maximum of TWO A4 pages for your newspaper article. You must format it according to the newspaper format. Feel free to put in any picture. You can also submit a maximum of ONE page for your reference list. Please submit your newspaper article and reference list (both hard and soft copies) at the beginning of the last class on October 26, 2005. All newspaper articles will be posted on the Webraft for revision purposes. You will also be given a maximum of 15 minutes to present your report. Please note that all students should participate in the presentation.

ABOUT THE AUTHOR

Nena Lim joined the Department of Accounting and Business Information Systems at University of Melbourne in January 2005. She holds her Ph.D. from University of Queensland. She also has an M.S. in Computer Information Systems from Georgia State University and an M.A. in Accounting & Finance from Lancaster University. Her work focuses on innovation diffusion, Internet security, and digital piracy.

.

Communications of the Association for Information Systems

ISSN: 1529-3181