Demonstrating Operating System Principles via Computer Forensics Exercises

Kevin P. Duffy
ISOM Department
Raj Soin College of Business
Wright State University
Dayton, OH 45435
kevin.duffy@wright.edu

Martin H. Davis, Jr.
Vikram Sethi
Institute of Defense Studies and Education
075 Allyn Hall
Wright State University
Dayton, OH 45435
martin.h.davis@wright.edu vikram.sethi@wright.edu

ABSTRACT

We explore the feasibility of sparking student curiosity and interest in the core required MIS operating systems course through inclusion of computer forensics exercises into the course. Students were presented with two in-class exercises. Each exercise demonstrated an aspect of the operating system, and each exercise was written as a computer forensics investigation. Students were asked to indicate their perception of the practicality of the course material before and after completing the exercises. Based upon a t-test, we conclude that students find the course material to be of greater practical significance when course materials are linked to forensics topics.

Keywords: Operating Systems, Computer Forensics, Class Exercises, MIS Major

1. INTRODUCTION

During ICIS (International Conference on Information Systems) 2005, a breakfast meeting for department heads was held. An agenda item for the breakfast was that of discussing the current MIS major curriculum at each of the represented schools, as well as problems related to changes and/or innovations in the curriculum. As a follow-up to this breakfast meeting, an email summary of a roundtable discussion at the conference was distributed to IS department heads who had attended the meeting (Robbert, 2006). The summary noted that IS is not perceived as appealing as other majors, and that the major needs better and more creative marketing to attract students. (The entire text of the roundtable discussion summary appears in the appendix to this paper.)

Educators often struggle to involve students in course materials and class discussions. Unfortunately, students perceive some material as dry or more remote. Although the operating system is an integral component of a computer-based information system, for many MIS majors the study of operating systems falls into this "dry" category, as the course content is perceived as being "too theoretical" in nature. The apparent tedium of this material has the effect of discouraging students from continuing in the MIS major (this required course is offered early in the undergraduate MIS major, and serves as a prerequisite to subsequent offerings in the major). In addition, the IS job market has slowed in recent years (Sandvig, Tyran, and Ross, 2005; Robbert, 2006), which has also had a downward impact on the desirability of MIS as a major. Hence, we wanted to discover if altering the explanation and presentation of some of the course topics might work to raise student interest in the course and retain them in the MIS major.

Presenting MIS as a major that contains a potential crime fighting tool (the operating systems course) may help attract students to the major. Discussing an episode of "CSI" (Crime Scene Investigation) or "Law and Order" within an

operating systems course may seem out of place at first. However, providing students with an exciting and practical application for the material under discussion in the classroom may encourage them to become more involved with the topic, ultimately leading toward greater mastery of the course material and greater retention of students in the MIS major.

Computer crime is increasing, thanks in large part to the Internet and the proliferation of home computers. Hence, this study has been undertaken to determine whether gearing explanations of operating system functionality around forensic discovery might be beneficial in teaching the material in the core, required operating systems course. Specifically, we examine whether incorporating computer forensics examples into the explanation of how an operating system works might spark student interest. In other words, our first motivation for this work is that computer forensics exercises may reinforce the material covered in class while serving to pique student interest.

A second motivation stems from work which explores the role of cognitive absorption in an MIS technology adoption (Agarwal and Karahanna, 2000). Agarwal and Karahanna (2000) investigate the phenomenon of student subjects 'losing track of time' when interacting with technology in an interesting fashion (the technology interaction was that of surfing the Web). In defining and describing the construct of cognitive absorption, Agarwal and Karahanna note (p. 667) that its theoretical bases "derive from three closely inter-related streams of research: the personality trait dimension of absorption, the state of flow, and the notion of cognitive engagement." Engagement is defined (Agarwal and Karahanna, 2000, p. 669) as including interest, curiosity and focus on a particular task.

Several of the dimensions included within the researchers' definition of cognitive absorption may apply to classroom settings:

- "focused immersion, or the experience of total engagement where other attentional demands are, in essence, ignored;
- "heightened enjoyment, capturing the pleasurable aspects of the interaction;
- "control, representing the user's perception of being in charge of the interaction; and
- "curiosity, tapping into the extent the experience arouses an individual's sensory and cognitive curiosity…" (Agarwal and Karahanna, 2000, p. 673).

Future work in this stream of research may provide insights which help to strengthen the delivery of course topics to our students. Further, utilizing computer forensics in an operating systems course may provide us with an avenue of investigation into the theoretical construct of cognitive absorption.

The paper proceeds as follows. We first provide an introduction to computer forensics. Following this, we describe an exercise that was incorporated into coursework as a "hands-on" experience for students enrolled in a core, required operating systems course. Finally, we describe the reaction of the students to the exercise, including instructor and student comments.

2. FORENSICS IN BRIEF

The mention of forensics likely brings to mind television dramas centered around murder scenes or surgical procedures conducted by a coroner. However, a growing specialization involves retrieving information from a computer system. Today's computer forensic examiner may work alongside law enforcement, retrieving hidden or deleted information from a home computer system (Richard and Roussev, 2006; The Economist, 2005). This information may range from deleted files (or pieces of deleted files) to existing documents stored on a hard drive or other storage media (Hosmer, 2006; Kay, 2006). Alternatively, the forensic examiner may search for information that identifies Web browsing behavior (Miller, 2007). In addition, computer forensics cases can occur within organizations (The Economist, 2005; Carrier, 2006). Boyle (2005, p. 39) commented that, although the underlying crimes seem vastly different from one another, "the trials of Scott Peterson, the BTK serial killer, Enron, and Merck's Vioxx have in common … [that] all have hinged, or will hinge, to some degree on digital evidence – e-mails, documents, web pages, pictures – procured from an individual's laptop or off a corporate network." Mercuri (2005) provides a list of cases ranging from an examination of accounting information, involving possible damage to computer records by an employee, through an examination of photographs to determine whether any alterations had taken place (Mercuri, 2005). Hosmer (2006) states that computer forensics have become so important to today's organizations that it is the corporate world, rather than the legal world, which is prompting the development of new forensic tools.

Organizations and individuals now interact with computers and information systems to a greater extent than ever before (Computer Industry Almanac, 2007). As computers have proliferated, the potential for computer crimes (such as email fraud, child pornography, sexual predators, identity theft, and illegal drug trafficking) has grown (Johnstone, 1996; Lloyd, 2004).

Consider the case of on-line chat rooms. Evidence suggests that Internet chat room popularity is due, in part, to its potential for anonymous interaction (Browne, 1997; Coffee, 2000; Traynor, 2005), since chat room participants are separated spatially. Separation and anonymity allow many chatters to create fictional characteristics and traits when interacting with others in the room. The anonymity which the Internet affords, coupled with the potential for a fictional identity, have created fertile ground for predators. (News stories describing the work of undercover officers staging Internet "sting" operations aimed at exposing and apprehending online sexual predators have become common (Globbe, 1995; McClellan, 2004; Shales, 2006).

The Internet has demonstrated that the computer is an ideal tool for communicating. What many users fail to realize, however, is that traces of conversations, emails, and other documents remain behind and often return to haunt their authors and recipients. Likewise, chatters believe that no trace is left behind once a participant has left the chat room and shut down their machine. Such traces, which often become critical evidence in court proceedings, can be uncovered – or recovered – through the use of computer forensic techniques (Boyle, 2005; "Digital Doubts," 2004).

Law enforcement agencies may rely upon forensic evidence in legal proceedings, such as in a court of law. Thus, the forensic examiner will exercise great care in ensuring that a forensic search or discovery does not alter or destroy any materials ("Digital Doubts," 2004; Swartz, 2005). The chain of custody for digital evidence is crucial to the examiner. Each step taken during a forensic examination must be fully and carefully documented and replicated if necessary. Boyle (2005, page 39) notes that performing a forensic analysis to recover evidence of digital crime may be described as "CSI in your hard drive."

In this paper, we adopt the definition of forensics as "the use of science and technology to investigate and establish facts in criminal or civil courts of law" (dictionary.com, 12/08/2007). By extension, we define computer forensics as "the application of specialized investigative and analytic techniques to identify, collect, examine and preserve data from computer systems or networks so that it may serve as evidence in a court of law" (Kay, 2006, p. 49). This definition is consistent with the usage found in the literature (Stephenson, 2003).

Applying computer forensics techniques depends upon a computer's operating system (Carrier, 2005; Richard and Roussev, 2006); forensic examiners are able to recover evidence by exploiting their knowledge of how computer operating systems function. Non-technical, untrained users may not realize that deleting a file or an email message will not *really* delete or remove all traces of it. Instead, a delete operation will render the file invisible, but still accessible via recovery tools, until it is overwritten by a new file. More savvy users may attempt to hide information by writing to file slack space. (Because operating systems allocate "chunks" of disk space at a time for files, there is often unused space found between an end of file marker and the end of the allocated chunk; this is known as slack space.) Forensic examiners are able to recover "ambient data" from places such as these. The examiner will also be able to retrieve information from the Windows swap file, as well (Castelluccio, 2002).

3. THE CASE STUDIES: FORENSICS EXERCISES

Forensics techniques fit well with the goal of facilitating students' learning of operating systems materials. We believe that students will show greater interest in the subject material when forensics demonstrations are added to the operating systems course material. Computer forensics is becoming more common in court proceedings, and in organizations (Carrier, 2006; Hosmer, 2006; Miller, 2007). We believe that the visibility forensics receives, coupled with the demonstration of the operating system's functionality, will provide students with a sense of "heightened enjoyment" (Agarwal and Karahanna, 2000). Thus, we draw upon the increasing visibility of computer forensics as well as the discussion of cognitive absorption to express this belief in the form of the following hypothesis:

H_1: Forensic demonstrations will increase student perceptions of the practicality of the course content.

Classroom activities, or hands-on experiences, have frequently been utilized as a means of reinforcing the lessons from the text and lectures (DeRoma and Nida, 2004; Johnston and McAllister, 2008; Ndoye, 2003; Skamp, 2007; Yopp, 2006; Young, 2002). Experiential learning can heighten a student's appreciation for the course material. Further, when students have visited course materials on a hands-on basis, they are apt to complete a course with a more solid, in-depth appreciation for that material.

In our case study, the students were presented with a simple, introductory level exercise aimed at deleting, and then undeleting, a text file created with the simple Microsoft Windows Notepad editor. The operating systems course covers file structures and the associated topics of how the operating system allocates blocks of space for a file. Finally, it is noted to the students that deleting a file merely updates the file directory and marks the disk space as available but does not actually remove the file's contents from the storage media. The first exercise is aimed at illustrating this concept to the students.

3.1 Forensics/OS Scenario 1

Purpose: To demonstrate how knowledge of Operating System (OS) principles aids in understanding certain computer forensics topics.

Background: Deleting a file and releasing its disk space is not the same as erasing the contents of the file's space. Silberschatz et al. (2009, p. 423) notes that "To delete a file, we search the directory for the named file. Having found the associated directory entry, we release all file space, so that it can be reused by other files, and erase the directory entry." However, only the directory entry is erased. The file's space on the secondary storage most likely is not erased. Therefore, even though the file was "deleted," its contents will remain on the secondary storage until overwritten.

Although the user may think that the file has been deleted, the contents of the file can still be recovered.

Course Activity: In MIS 305 ("Business Operating Systems"), students are exposed to the manner in which the operating system allocates storage space for files, as well as to the manner in which "deleting" a file does not *actually* delete the file. After learning these concepts, the students are instructed to create a short file, to save the file to the C: drive, and to then delete the file. Once the file has been deleted, students utilize a simple file recovery program (e.g., "SoftPerfect File Recovery," http://www.softperfect.com/products/filerecovery/) to "un-delete" the file. Students then compare the "undeleted" file to a saved copy of the original file. The following steps will be performed.

1. Create a text file (with a file extension of .txt) using Microsoft Notepad.
2. Enter the first paragraph of chapter 10 (page 421 of the Silberschatz text) as the contents of the file.
3. Save the file to the C: drive as "Para1.txt."
4. Save a second copy of the file with a different name: "Para1a.txt."
5. Using the "My Computer" utility, browse to find the file "Para1.txt" on the C: drive.
6. Delete the file "Para1.txt."

7. Open the Recycle Bin. Click to empty the Recycle Bin.
8. Utilizing the file recovery program, "undelete" or recover, the file "Para1.txt."
9. Open the recovered file, "Para1.txt" and the duplicate file "Para1a.txt" in side by side notepad windows.
10. How do these 2 files compare to one another? What does this exercise demonstrate regarding the potential outcomes of deleting a file from the computer?

Outcome: Before completing this exercise, students study the theoretical concepts of files, file structures, and disk space allocation. As a result of this exercise, students form a concrete connection from the theoretical to the actual by realizing that a file's contents remain on the hard drive after the file has been deleted. Because the contents remain on the hard drive, the file can be retrieved, or undeleted.

Students enrolled in the core MIS operating systems course were presented with a second scenario involving examining the "swap file," a topic that is included in the course. The swap file (also known as a "page" file), in a Windows operating environment, permits the system to act as though it has more main memory (also known as RAM) than it actually does have (a concept called "virtual memory"). To accomplish this feat, the operating system "swaps," or copies, the contents of memory to the "swap file" (located on the hard disk) until these contents are needed again, thus freeing up memory for other contents ("Swap file," www.Webopedia.com, 05/18/2009). This swap activity has an important ramification for the persistence of information stored in a temporary storage area such as main memory. A Microsoft publication, "The Information Worker's Security Handbook," points out that user data exists in numerous places on the computer: "Information you have deleted may still exist in memory (if the computer has not been turned off) or in virtual memory (the page file or swap file on the hard disk)" (Microsoft, 2004, p. 39). Additionally, numerous authors mention that an examination of the swap file is a key digital forensic technique (Miller, 2007; Castelluccio, 2002). To bring the concept of a "swap file" to life, students were presented with the following exercise:

3.2 Forensics/OS Scenario 2

Purpose: To show how knowledge of Operating System (OS) principles aids in understanding why certain computer forensics techniques are useful.

Background: Virtual memory is the illusion provided to an application program that it has as much memory available as it wants, i.e., the *address space* of the application ranges from 0 – N-1, where N is some arbitrarily large number whose value is determined by the fundamental design of the computer's processor. Virtual memory is implemented by *paging* (sometimes called swapping) various pieces (called *pages*) of the address space from the hard drive to RAM and vice versa. The paging is managed by the OS – typically, neither the user nor the application programmer has any knowledge or control over what pages in the application's address space are resident in RAM at what time.

As various application programs are loaded, executed, and exited by the user, the contents of the paging file (named *paging.sys* in Windows 2000) will change, but remnants of what an application program was doing can persist in the paging file for an indefinite period of time, even when the computer is shut off and the contents of RAM are lost. Thus, one computer forensics technique is to examine the contents of the paging file to determine what activities the user was previously engaged in.

Course activity: In MIS 305 ("Business Operating Systems") students are exposed to the concept of virtual memory and the mechanisms used to implement it. After learning these concepts, the students will engage in the following activity. Each student will be provided a copy of a Windows paging file and an appropriate text editor/searching tool. Using the tool and standard Windows tools, the student will perform the following steps:

1. Determine the size of the paging file.
2. Note the relationship between the file's size and the size of the RAM on the computer from where the paging file came.
3. Note the file's creation, modification, and access dates/times.
4. Examine the contents of the file, and make note of any "unusual" text strings found within the file.
5. Search the hard drive of the computer from where the paging file came for occurrences of these "unusual" text strings in other files.
6. Speculate as to the meaning of these text strings and the activity that generated them.

Outcome: Before engaging in this activity, the student will have been exposed to the theoretical concepts and mechanisms behind virtual memory. After engaging in this activity, the student will have formed a concrete connection from the theoretical to the actual by realizing that the paging file does indeed contain a record of what various application programs did while executing. Thus, the student's knowledge of OS principles will aid him in understanding why a particular computer forensics technique works.

4. RESULTS

Before beginning the first exercise, students were asked to respond to the following statement: "While learning about computer operating systems, I can envision myself utilizing the course content." The question was presented to the students as a 7-point Likert-type scale (1= strongly disagree through 7 = strongly agree). (The question and its possible responses was modified from the instrument presented in the work of Agarwal and Karahanna (2000)). At the end of the class period (exercise 2 was also included in the class period), students were asked to respond again to the question. A paired t-test was conducted; the results of the t-test allow us, given the data collected, to reject the null hypothesis ($\alpha = 0.05$; $\rho < 0.00$; see Table 1). Hence, we conclude that the inclusion of forensics demonstrations in the operating systems course will raise student perceptions of the practicality of the course material.

Forty-six students completed the forensics exercises detailed above. Several students shared, via email, unsolicited comments concerning the forensics exercises. These comments add support to our belief that the computer forensics examples will work to increase student interest in operating systems as well as in the MIS major. For example, one respondent noted that "…these are the kinds of activities that MIS students envision when they sign up for MIS classes … the more a student can interact with the OS in the way that your activity requires, the more interesting and useful the experience will be. Most people will remember very little about the class that they had to sit through and take notes from lectures and Powerpoints [sic], but when they do something hands-on that they can take with them and show others, it is far more lasting and useful." Another student stated that "Wow, the new addition to the class sounds really interesting." One very strong comment stated that on "… a personal note, I am glad that you are bringing this kind of participative activity to this class. To be able to relate a practical exercise to very mundane theoretical concepts. You will allow people to explore, think, and develop a stronger understanding of the applied sciences involved in computer operating systems." The receipt of the unsolicited emails presents further evidence that the exercise did indeed catch the students' attention and is something that they will remember. Further, we note that the enthusiasm that these students conveyed in their email far exceeds the excitement demonstrated over other course homework assignments.

	Pre-Test Response	**Post-Test Response**
Mean	4.9782	6.1086
Std. Dev.	1.5127	1.0588
df	45	
t Stat	-4.3589	
P(T<=t) one-tail	3.74987E-05	
t Critical one-tail	1.679427393	
P(T<=t) two-tail	7.49973E-05	
t Critical two-tail	2.0145103359	

Table 1. t-Test Statistics

Further student feedback was gained from the class discussion, according to the course instructor. Before completing the second exercise (exercise two is an examination of the windows page file), the instructor reported that students thought that when they stopped a particular program or application, it would not be possible to determine what the program had been doing unless the program purposely had saved data on the hard drive. Initially, the instructor mentioned, students found it "strange" to be opening a 750 MB file, since opening this file took much longer than the opening speed which they were accustomed to experiencing when opening a typical Word or PowerPoint file.

Students experienced an adjustment period of a few minutes once the page file had been opened with the text editor. Most of the students were very baffled by the fact that they were looking at strings of normal, readable words and phases interspersed with strings of apparently random characters. Once the students had adjusted to the strange appearance of the file, their next step was to become familiar with how to use the text editor to search for strings in the file. The instructor, at this point, suggested that they think about what activities they, as students, perform while on a computer (e.g., browsing the Web, writing papers, composing e-mail, etc.) and what kinds of words and/or phrases they might encounter or write during such activities. (The instructor pointed out to the students that the forensics investigator might not necessarily "know" what she was looking for when examining the contents of a swap file.)

5. LIMITATIONS OF THIS RESEARCH

One drawback to the exercises is that the size of the class (46 students) did not permit us to collect data for statistical analysis in the arena of cognitive absorption (Agarwal and Karahanna (2000) conduct a path analysis utilizing a much larger sample of subjects than the 46 participants in this study). Because any statistics we present would lack statistical power, we are unable to support any definite conclusions regarding the effectiveness of the exercises in demonstrating and explaining the functioning of an operating system, and a possible relationship to cognitive absorption. However, multiple offerings of the course may provide, in time, a resource for future data collection and more in-depth research.

6. DISCUSSION AND CONCLUSIONS

Incorporating computer forensics topics into the operating systems course has given students a greater appreciation for the role and functioning of a computer's operating system. In addition, the students' involvement with the course material has grown. Once the students overcome the immediate barrier of how to look through the file, and what to look for, they became intensely engaged in the exercise. When a student happened upon a word or phrase that was of interest, the student then became fascinated by what else could be found. (In this particular page file, students were able to find words and phrases that related to shopping at online retailers, warranty information, etc.) Several of the students expressed utter amazement that some of the information found in the page file was several years old (one student found phrases dated from 5 years prior to the current date that were related to having searched online at an electronics store). Once the time allotted for the exercise concluded, the instructor noted that it was difficult for the students to quit searching and join the class discussion.

The results of the initial exercises were encouraging. Based upon student reaction to the forensics exercises, we hope to incorporate them into the operating systems course. In addition to the comments from the class discussion and those received via email, another student approached the instructor to discuss an independent study in computer forensics. One deliverable from the proposed independent study was allowing the student to demonstrate his grasp of forensics by suggesting computer forensics exercises or scenarios for other core MIS courses (i.e., database, telecommunications, networking).

As individuals, organizations, and societies become more adept at using computers and more reliant upon computers

for daily transactions, the possibility of fraud or crime continues to grow. Although computer forensics is currently viewed as a relatively young investigative technique, its use is likely to increase as computerization increases. In discussing the future of forensics, Richard and Roussev (2006) note that as computing equipment grows larger, performing forensics tasks will become more and more cumbersome.

Further, it is worth noting that a computer forensics examiner may work with various operating systems to expose and recover data. Studying the Linux operating system and running Windows and Windows applications from within it would allow students to compare the operation of one OS versus another. Therefore, as an additional exercise toward understanding other operating systems, students may apply the same forensic examples to Linux. Introducing students to forensics, its importance, and its purpose may serve the dual purpose of solidifying student interest in the required operating systems course and introducing a potential career within the MIS field. Alternately, other courses or disciplines may address other aspects of the broader domain of digital forensics topics. Discussing these different disciplines and how they utilize or rely on forensics will demonstrate to students how far-reaching and broad a topic is digital forensics.

We are optimistic that computer forensics may provide us with an appropriate venue for exploring cognitive absorption in the classroom. Additional effort will be required in order to transition the course from its present state to a course where the examples and illustrations are geared around computer forensics-type investigations. One idea is to structure a course-long scenario where student assignments involve forensics to uncover usage activities and patterns from a suspect personal computer. Also, because the course is offered within a University environment, care must be taken to safeguard our students in the classroom. These hurdles notwithstanding, our preliminary glimpse into the fit between operating systems and computer forensics has convinced us that this idea may be pursued fruitfully.

Ultimately, our goal is to provide students with the strongest understanding possible of the various components which make up an MIS major. Placing additional emphasis on student mastery of the concepts taught within the operating systems course will serve to increase the knowledge base which our graduates take into the workplace.

7. ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their extremely helpful suggestions of revisions to this paper. The suggestion of a course-long scenario, which is mentioned in the conclusion, stems from a reviewer's comment.

8. REFERENCES

Adelstein, F. 2006. "Live forensics: Diagnosing your system without killing it first," Communications of the ACM, Vol. 49, No. 2, pages 63-66.

Agarwal, R. and Karahanna, E. 2000. "Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage," MIS Quarterly, Vol. 24, No. 4, pages 665-694.

Boyle, M. 2005. "The latest hit: CSI in your hard drive," Fortune, Vol. 152, No. 10, page 39.

Browne, S. 1997. "The chat room as a 'third place,'" Brandweek, Vol. 38, Issue 15, page 24.

Carrier, B. 2005. File System Forensic Analysis. Upper Saddle River, NJ: Addison-Wesley.

Carrier, B. 2006. "Risks of live digital forensic analysis," Communications of the ACM, Vol. 49, No. 2, pages 56-61.

Castelluccio, M. 2002. "Computer forensics – A cheat sheet," Strategic Finance, Vol. 84, No. 2, pages 59-60.

Coffee, P. 2000. "Who knows the real you?" eWeek, Vol. 17, Issue 45, page 61.

Computer Industry Almanac & eTForecasts. 2007. "Leading countries by number of computers-in-use," pages 36-38.

DeRoma, V. and Nida, S. 2004. "A focus on 'hands-on,' learner-centered technology at The Citadel," Tech Trends: Linking Research & Practice to Improve Learning, Vol. 48, Issue 5, pages 39-43.

Dictionary.com. Definition of "forensics," retrieved 12/08/2007, www.dictionary.com.

"Digital Doubts," 2004, Communications of the ACM, Vol. 47, No. 4, pages 9-10.

The Economist. 2005. "Dusting for digital fingerprints," Economist, Vol. 374, Issue 8417, March 12, 2005, pages 32-33.

Globbe, D. 1995. "Online seduction sting," Editor & Publisher, Vol. 128, Issue 21, page 11.

Hosmer, C. 2006. "Digital evidence bag," Communications of the ACM, Vol. 49, No. 2, pages 69-70.

Johnston, A.N.B. and McAllister, M. 2008. "Back to the future with hands-on science: Students' perceptions of learning anatomy and physiology," Journal of Nursing Education, Vol. 47, No. 9, pages 417-421.

Johnstone, H. 1996. "Computer crime skyrockets." Asian Business, Vol. 32, Issue 12, page 18.

Kay, R. 2006. "Computer Forensics," Computerworld, Vol. 40, Issue 16, April 16, 2006, page 49.

Lloyd, T. 2004. "Be prepared for cyber-crime." IT Training, April 2004, page 14.

McClellan, S. 2004. "Controversy surrounds sex-predator sting," Broadcasting & Cable, Vol. 134, Issue 12, page 14.

Mercuri, R.T. 2005. "Challenges in forensic computing," Communications of the ACM, Vol. 48, No. 12, pages 17-21.

Microsoft Corporation. 2004. The Information Workers' Security Handbook. download.microsoft.com/ download/ 2/6/6/266a2a52-8fd5-4e26-b7c0-c58ef55c021/Information %20Workers%20Handbook.doc. Accessed May 5, 2009.

Miller, R. 2007. "The truth is in there," EContent, Vol. 30, Issue 2, pages 38-43.

Ndoye, A. 2003. "Experiential learning, self-beliefs and adult performance in Senegal," International Journal of Lifelong Education, Vol. 22, No. 4, pages 353-366.

Richard III, G.G., and Roussev, V. 2006. "Next-generation digital forensics," Communications of the ACM, Vol. 49, No. 2, pages 76-80.

Robbert, M.A. 2006. ICIS roundtable.doc: Summary of curriculum discussion at ICIS department heads breakfast, email communication, dated January 8, 2006.

Sandvig, J.C. Tyran, C.K. and Ross, S.C. 2005. "Determinants of graduating MIS student starting salary in boom and bust job markets," Communications of the Association for Information Systems, Vol. 16, pages 604-624.

Shales, T. 2006. "Entrapped in Datelineland," Television Week, Vol. 25, Issue 10, page 27.

Silberschatz, A.; Galvin, P.B.; and Gagne, G. 2009. Operating System Concepts (8th Ed.). John Wiley & Sons, Inc.

Skamp, K. 2007. "Conceptual learning in the primary and middle years: The interplay of heads, hearts and hands-on science," Teaching Science – The Journal of the Australian Science Teachers Association, Vol. 53, No. 3, pages 18-22.

Stephenson, P. 2003. "Structured investigation of digital incidents in complex computing environments," Information Systems Security, Vol. 12, Issue 3, pages 29-38.

Swartz, N. 2005. "U.S. Justice Department releases digital evidence guidelines," The Information Management Journal, Vol. 39, Issue 1, page 10.

"Swap file," and "swap," www.webopedia.com/TERM/s/swap_file.html and www.webopedia.com/TERM/s/swap.html, retrieved on May 18, 2009.

Traynor, M. 2005. "Anonymity and the Internet." Computer & Internet Lawyer, Vol. 22, Issue 2, pages 1-16.

Yopp, R. H. 2006. "Enhancing hands-on science experiences with informational texts: Learning about pine cones," Science Activities, Vol. 43, Issue 3, pages 31-34.

Young, M.R. 2002. "Experiential learning = hands-on + minds-on," Marketing Education Review, Vol. 12, No. 1, pages 43-51.

AUTHOR BIOGRAPHIES

Kevin P. Duffy became an Assistant Professor of MIS in the ISOM Department in September 2004. He completed his doctoral studies in Management Information Systems at the Florida State University. He completed a BA degree from Eckerd College in Literature in 1978, and an MA degree in Literature from the University of Pittsburgh in 1982. He completed an MSIS at the University of Pittsburgh in 1992. His publications have appeared in journals such as Decision Support Systems, the Journal of Asia-Pacific Business, the Air Force Journal of Logistics, the International Journal of Public Administration, and the Encyclopedia of Information Systems. Dr. Duffy is the Executive Director of the EDAptive Computing Center for Research in Business Process Management.

Martin H. Davis, Jr. is a Project Manager for the Institute of Defense Studies and Education at Wright State University. He has also served as an adjunct professor and coordinator of masters programs for the ISOM Department. Prior to his academic career, Dr. Davis worked for small businesses which specialized in computer and networking technologies. He earned a B.S. in Space Science and a B.S. in Physics from the Florida Institute of Technology, an M.S. in Engineering Science from the University of Tennessee Space Institute, and the Ph.D. in Computer Science from the Georgia Institute of Technology. His research interests include the use of technology in a learner-centric classroom and how small businesses can cost effectively utilize parallel computing to improve their efficiency and competitiveness.

Vikram Sethi joined the Raj Soin College of Business in June 2003 in the capacity of Chair of the Information Systems and Operations Management Department. Prior to this time, he held faculty positions at the University of Texas at Arlington, and at Southwest Missouri State University. He holds a Ph.D. in Management Information Systems from the University of Pittsburgh. His research interests include data warehousing, business process reengineering, transnational information systems, and organizational transformation. His publications have appeared in numerous journals, including Omega, Focus on Change Management, Journal of Global Information Technology Management, and Journal of Management Information Systems. Dr. Sethi currently serves as Advisor to the Dean for Corporate Relations. Dr. Sethi is Director of the Institute for Defense Studies and Education.

APPENDIX 1

Roundtable Discussion Summary provided by M.A. Robbert
Sent to MIS Department Heads as an email communication
Dated January 8, 2006.

Our table discussed what was possible within the current major structure. Reviewing the number of courses in the major, we discovered the range in business schools was from 4 required courses + 4 electives + a project to 9 required + 1 elective. 12 required courses + 7 electives were available to majors outside business schools and engineering schools had 10 + 2 requirement. The number of courses permitted in the major, and the number of electives greatly effects the flexibility in the curriculum.

We discussed BPM as the gateway to the major. Positives, (understand the problem, get an overview), and negatives, (students not ready, will not understand), were considered. BPM offered by management department was considered boring. Potential for BPM to be an exciting entry into IS major. No suitable software for introductory BPM course available.

Other courses were discussed. It was agreed Java should be taught by CS department if possible. Java can be a later course or an elective rather than the first course. Algorithms using Alice was suggested to maintain student interest. Different approaches such as a portfolio or using a PDA to support course work were deliberated but were considered appropriate only for particular schools.

Lower enrollment in IS major is universal. IS major no longer considered sexy. We must define what IS is and show that jobs are available. Business analysts' positions are available and are not being sent off-shore.

Overall the discussion was positive. We felt that the IS major needed to be marketed better and presented to students more creatively. Using BPM as the first course should be considered.

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096