ISSN: 1545-679X

Information Systems Education Journal

Volume 7, Number 35 http://isedj.org/7/35/ April 27, 2009

In this issue:

Offering a Digital Forensics Course in Anchorage, Alaska

Alpana M. Desai
University of Alaska Anchorage
Anchorage, Alaska 99508 USA

David Fitzgerald
University of Alaska Anchorage
Anchorage, Alaska 99508 USA

Bogdan Hoanca
University of Alaska Anchorage
Anchorage, Alaska 99508 USA

Abstract: Digital forensics (DF) has become important due to a sharp increase in computer crimes and an acute shortage of trained digital forensics personnel. Cyber crimes may involve crimes committed across several states or across international borders and require the cooperation and collaboration of various local, state, federal, and international law enforcement agencies. Many times local and state, law enforcement agencies do not have investigators trained or skilled in investigating cyber crimes due to lack of IT skills. Alaska is one of only two non-contiguous states of U.S.A. Anchorage is the most populous city of Alaska with more than 50% of the state's population. It has eight law enforcement agencies but a severe shortage of law enforcement officers with the necessary technical expertise to investigate computer crimes. In this paper, we present the planning and design of a digital forensics course that meets the needs of local law enforcement agencies, interested students, and members of the local community. The issues involved in offering such a course are presented. The infrastructure needed is explored with concluding observations.

Keywords: digital forensics, computer forensics, curriculum, security

Recommended Citation: Desai, Fitzgerald, and Hoanca (2009). Offering a Digital Forensics Course in Anchorage, Alaska. *Information Systems Education Journal, 7* (35). http://isedj.org/7/35/. ISSN: 1545-679X. (A preliminary version appears in *The Proceedings of ISECON 2006:* §5114. ISSN: 1542-7382.)

This issue is on the Internet at **http://isedj.org/7/35/**

The **Information Systems Education Journal** (ISEDJ) is a peer-reviewed academic journal published by the Education Special Interest Group (EDSIG) of the Association of Information Technology Professionals (AITP, Chicago, Illinois). • ISSN: 1545-679X. • First issue: 8 Sep 2003. • Title: Information Systems Education Journal. Variants: IS Education Journal; ISEDJ. • Physical format: online. • Publishing frequency: irregular; as each article is approved, it is published immediately and constitutes a complete separate issue of the current volume. • Single issue price: free. • Subscription address: subscribe@isedj.org. • Subscription price: free. • Electronic access: http://isedj.org/ • Contact person: Don Colton (editor@isedj.org)

EDSIG activities include the publication of ISEDJ and JISAR, the organization and execution of the annual ISECON and CONISAR conferences held each fall, the publication of the Journal of Information Systems Education (JISE), and the designation and honoring of an IS Educator of the Year. • The Foundation for Information Technology Education has been the key sponsor of ISECON over the years. • The Association for Information Technology Professionals (AITP) provides the corporate umbrella under which EDSIG operates.

Offering a Digital Forensics Course in Anchorage, Alaska

Alpana M. Desai
afamd@uaa.alaska.edu

David Fitzgerald
afdaf@uaa.alaska.edu

Bogdan Hoanca
afbh@uaa.alaska.edu

Department of Computer Information Systems
University of Alaska Anchorage
Anchorage, Alaska 99508 USA

Abstract

Digital forensics (DF) has become important due to a sharp increase in computer crimes and an acute shortage of trained digital forensics personnel. Cyber crimes may involve crimes committed across several states or across international borders and require the cooperation and collaboration of various local, state, federal, and international law enforcement agencies. Many times local and state, law enforcement agencies do not have investigators trained or skilled in investigating cyber crimes due to lack of IT skills. Alaska is one of only two non-contiguous states of U.S.A. Anchorage is the most populous city of Alaska with more than 50% of the state's population. It has eight law enforcement agencies but a severe shortage of law enforcement officers with the necessary technical expertise to investigate computer crimes. In this paper, we present the planning and design of a digital forensics course that meets the needs of local law enforcement agencies, interested students, and members of the local community. The issues involved in offering such a course are presented. The infrastructure needed is explored with concluding observations.

Keywords: **digital forensics, computer forensics, curriculum, security**

1. INTRODUCTION

The Computer Information Systems department at University of Alaska Anchorage (UAA) is planning to offer a course in Digital forensics, starting in fall 2007. This paper outlines the course plan, the key decision points faculty made in the planning of the course, and the opportunities for collaboration with local law enforcement, local businesses and other academic departments at UAA.

Digital forensics is the application of the scientific method to digital media in order to establish information for judicial review. This process often involves investigating computer systems to determine their usage for illegal or unauthorized activities. Mostly, digital forensics experts investigate data storage devices, either fixed like hard disks or removable like compact disks and solid-state devices. Digital forensics experts:

- Identify sources of documentary or other digital evidence.
- Preserve the evidence.
- Analyze the evidence.
- Present the findings.

Procedures in digital forensics adhere to standards of evidence that are admissible in a court of law, (Wikipedia, n. d.).

There are about 100 colleges and universities in USA that offer undergraduate and graduate courses in digital forensics, (Swartz, 2006). Due to the presence of several local, state, and federal law agencies and military based locally in Anchorage, Alaska, there is an increased need and interest in digital forensics. There is a shortage of experienced or certified professionals with technical expertise and experience in investigative and forensics examination procedures. There are faculty members qualified to teach a digital forensics course and finally there is lab infrastructure for hands-on projects. These are some of the reasons for offering a digital forensics course in Anchorage, Alaska. In this paper, we first conduct an exploratory study to determine the factors that justify offering a digital forensics course at the University of Alaska Anchorage (UAA). The methodology used is to conduct a case study to identify factors that justify offering a course in digital forensics and to create a framework for use by any college or university that aims to offer a similar course. We conduct an exploratory study by considering the case of Mississippi State University (MSU). MSU is a Center for Academic Excellence (CAE) in Information Assurance and offers courses in digital forensics at the introductory and advanced level. It is also a mentor to UAA. MSU was the best choice for conducting this study due to accuracy in data collected for determining the factors and for creating a framework, and for assessing these factors in the case of UAA.

> *The next (third) section provides the details of the study conducted for MSU and presents an overview of the current situation in cyber crimes investigation in Anchorage, Alaska. It identifies the important factors that justify offering a digital forensics course and provides the framework of important factors. The fourth section presents the course content for this course. The following sections discuss the infrastructure required and collaboration plans to offer such a course. The paper concludes with observations and recommendations for future work.*

2. EXPLORATORY STUDY

MSU has been designated as a Center of Academic Excellence in Information Assurance Education by the National Security Agency (NSA) since 2001, (National Security Agency, n. d.). MSU offers both undergraduate and graduate DF courses. According to D. Dampier, (personal communication, July 27, 2006), the Forensics Training Center at MSU also offers three-day, short courses in digital forensics to law enforcement officers from across the southeastern U.S.A.

The campus of MSU is located in Starkville, which is in Oktibbeha County, Mississippi. The population of the city of Starkville as of the 2000 census was 21,869, which is less than 10% of Anchorage’s population. In contrast, as of the 2000 census, the population of the state of Mississippi was 2,844,658. The university dominates the city's economy, (Wikipedia, n. d.). There are four law enforcement agencies in Starkville. They are Starkville Police Department, Oktibbeha County Sheriff's Department, Mississippi State University Police Department, and Tri-County Narcotics Bureau. Local cyber crimes that have been investigated include embezzlement and computer theft. The faculty and students have assisted the local sheriff’s department with an embezzlement case and the MSU police department with a computer theft case by examining computer media for specific evidence, (D. Dampier, personal communication, July 27, 2006). FBI has only one field office in the entire state of Mississippi. This field office serves all the counties in the state and it is in Jackson, which is the capital of Mississippi.

Next, we consider the case of UAA and Alaska. There is an increased interest and need to offer a digital course in Anchorage, Alaska. Alaska has several federal, state, and local (Anchorage) law enforcement agencies. Federal Bureau of Investigation (FBI) has a field office in Anchorage. Fairbanks and Juneau each have a FBI resident agency. FBI's Field Offices are located in major cities throughout U.S.A whereas resident agencies are maintained in smaller cities and towns across the country, (Federal Bureau of Investigation [FBI], n. d.).

Forbes magazine ranks Anchorage as the 52nd best places for doing business in 2006, (Badenhausen, 2006). Anchorage is the most populous city of Alaska with a population of 348,600, having over 50% of the state’s population of 626,932. The likelihood of the gas pipeline being built and a large military base account for a steady influx in Anchorage. At the IT Exposition held in Anchorage on Oct. 20, 2005, special agent Alan Vanderploeg said that cyber crime is the Federal Bureau of Investigation's No. 3 priority, behind domestic and international terrorism, (Chandler, n. d.). The two units of Anchorage Police Department (APD) that are involved in investigating and analyzing computer crimes are the fraud unit and the computer crimes unit. Of about 1,500 reports that are received, the fraud unit is able to track about 200 cases according to priority. About 50 percent of the tracked cases involve some computer usage and 20 percent involve cyber crimes, (Chandler, n. d.). The computer crimes unit has only two full-time detectives that are involved in the analyses of the cyber crimes, (Chandler, n. d.). According to the supervisor of APD’s fraud and computer crimes units, Sgt. Walt Gilmour, the APD worked with the FBI on approximately 50 cases in 2004, (Chandler, n. d.). Cooperation of multiple law enforcement agencies is needed for smooth investigation of cases where the cyber criminals and their victims live hundreds or thousands of miles apart. This clearly shows that there is a shortage of experienced or certified professionals with technical expertise and experience in investigative and forensics examination procedures.

Next, we discuss another factor for offering digital forensics course at UAA. There are four educational institutions in Anchorage: University of Alaska Anchorage (UAA), Alaska Pacific University (APU), Charter College (CC), and Wayland Baptist University (WBU). UAA is the largest member of the University of Alaska System, with over 17,000 students and is in fact, the largest academic institution in the entire state of Alaska. Teaching a digital forensics course effectively involves offering hands-on laboratory exercises; hence taking an online version of this course will not be helpful to an interested student. A basic course in digital forensics is offered by CC in their associate’s degree program in network security, but none at the intermediate or advanced undergraduate level, (Charter College, n. d.). No digital forensics course is currently offered by APU or WBU. Two pilot versions (half-semester long) of this course have already been offered at UAA. One of the half-semester pilot versions of the DF course was taught by a UAA faculty who is a digital forensics examiner trained by AccessData and hence highly qualified. The other pilot version was taught by the director of the Forensics Training Center at the Mississippi State University (MSU). Offering such a course requires guidance and mentorship from universities that have qualified and experienced faculty and that have had a successful implementation of the course. This discussion establishes the importance of a qualified faculty to teach a digital forensics course.

Table 1: Important Factors

Factors	**Anchorage, Alaska**	**Starkville, Mississippi**
Number of law enforcement agencies	8	4
Existence of a FBI Field Office	Yes	No
Population	348,600	21,869
Number of law enforcement officers investigating computer crimes in the local police department	2	0
Number of Faculty Qualified to teach a DF course	1	1
Existence of lab infrastructure	Yes	Yes
Number of DF courses	0	3

Teaching digital forensics without hands-on exercises is not effective. Establishing labs for hands-on, in-class activities is of absolute importance for student learning. We explore the importance of lab infrastructure and steps for creating a lab that supports a digital forensics course in a separate section.

After analyzing results obtained from conducting the exploratory study, we identify the following important factors. Institutions that plan to offer a digital forensics course must consider these factors to assess the feasibility of offering such a course.

- Existence and a high number of law enforcement agencies
- Existence of a FBI Field Office
- Large Population
- Low number of law enforcement officers investigating computer crimes locally
- Existence of faculty qualified to teach a digital forensics course
- Existence of lab infrastructure

Table 1 compares these factors from the perspective of UAA and MSU. These factors influenced our decision to offer a full-semester undergraduate DF course at UAA.

The next section discusses the course outline that is being proposed for the new DF course.

3. COURSE OUTLINE

Premise: Worldwide, computer crimes are growing at a faster rate than the availability of trained digital forensics examiners required to investigate them. Law enforcement officials in most major cities across the United States report a growing backlog of pending cases. Here in Anchorage, Alaska, the police concentrate primarily upon child pornography and other criminal offenses. They have little or no time for civil litigation.

Digital forensics is somewhat different from other computer security issues in that it takes place after the violation has already been committed. However, the continued use of forensics procedures can help to deter future infractions.

Audience: Personnel from law enforcement at all governmental levels, IRS, Customs and Immigration, military, corporate security, and any individual interested in pursuing digital forensics as a career will benefit from this course.

Computer Lab: We foresee our lab patterned after that of Mississippi State wherein we can offer training to law enforcement officials as well as the students outlined above. Initially we will use the Forensic Toolkit (FTK) from AccessData. Eventually we would like to include Encase from Guidance Software, and possibly even ILook Investigator. We have already purchased a Logicube MD5 data-capturing unit and associated accessories.

4. KEY TOPICS

Law, investigations, and ethics: This topic deals with the definition of acceptable computer usage, computer crime, and electronic discovery. The Sarbanes-Oxley Act and other similar legislation have redefined many legal and ethical issues.

The history and future need for digital forensics: This topic examines how the subject of digital forensics has evolved and the growing need as the world becomes more and more computer literate. According to Anchorage Police Department officer Glen Klinkhart (email, July 22, 2006), "Information Security is a real science and a craft".

Search and seizure issues: This topic discusses the Fourth Amendment to the Constitution of the United States and contrasts the differences between criminal and civil investigations, and the different types of computer evidence.

Sources of electronic evidence: This topic investigates the different types of media that are a potential for evidence in an investigation. These items include the hard disks in the PC's, PDA's, and various storage media such as floppy disks, zip disks, etc. It is particularly essential that the students understand the possible dishonest capabilities of relatively newer devices such as USB drives, MP3 players, iPods, and other storage devices.

How hard drives, memory, operating systems, and file systems work: Because our college does not require a computer hardware course, students will be able to investigate the internal workings of a dismantled computer hard drive. This topic examines the details and differences in the various popular operating system (Windows, Apple/Mac, Unix/Linux), and the various file systems (FAT, NTFS, MFS, UFS, etc). It also explains how computers store data, how they process data, computer caching, virtual memory, disk free space, disk slack space, and the registry.

Common forensic tools: This topic compares and contrasts the most popular forensic tool software packages (FTK, Encase, and ILook) as well as many of the downloadable freeware and shareware investigative tools. The first lab Exercise supports the topic.

Passwords and encryption: This topic illustrates the various means of deducing users' passwords. We discuss the various types of encryption, and their strengths and weaknesses. We utilize FTK and other decryption software to "decrypt" files and passwords.

Testifying in court: This topic discusses the methods required to present cases successfully to the courts. The best evidence obtainable is of no use in a trial if the judge and jury do not understand the information presented to them. We explain the requisite guidelines for appearance, attitude, giving only the necessary information, and being prepared to answer questions from the opposing side. We give examples of how to keep your technical information in simple terms, and suggest visual aids that are understandable to most audiences. We intend to include the UAA College of Health and Social Welfare, Justice Center to assist in this topic.

Labs

Common forensic tools: The first Lab Exercise requires the students to install the FTK forensic software. We then perform an initial review of the FTK features.

Preparation for a forensic investigation: It is crucial that an investigator arrive at a suspected crime scene prepared. This second Lab Exercise requires the students to delineate the items that an investigator should bring with him/her to the site such as cameras, voice recorders, anti-static storage containers, etc., and they will be required to create a chain of custody form.

Evidence identification, preservation, and analysis: The third Lab Exercise tests the ability of the students to detect (in a controlled environment) the different types of articles that are a potential for evidence in an investigation. These items range from the physical media described under "Sources of electronic evidence" above, to printed and written documents including "sticky-notes".

Capturing, acquiring, and validating the data: In this fourth Lab Exercise the students utilize both the MD5 and a PC to capture and validate (through hashing), an image of a test "suspect" drive, then acquire the image utilizing the FTK software. We utilize and discuss the use of a "write-blocker". Because of the power of forensics tools, and the possibility of the students viewing "sensitive or inappropriate" information on a genuine drive acquired from an ex-user, we use a fabricated test drive. We discuss and implement the correct time zone information to corroborate actual file and message creation and modification times.

Extracting information from the data: As a continuation of the fourth Lab Exercise, the students narrow their focus and utilize the FTK software to extract specific information based upon pertinent search criteria. We discuss the various document and graphics file formats and the software packages that create them. This Lab also identifies and investigates the various components of email messages and attachments.

Analyzing the data: In the fifth Lab Exercise the students utilize the FTK software to analyze and assimilate the resulting search criteria from above to ascertain what information is pertinent to our specified case.

Documenting and reporting the case: This topic explains the documentation required to prove there was no tampering of the evidence. If there is the slightest chance of the case going to court, thorough documentation is critically important. The sixth Lab Exercise requires that the students are able to verify the chain of custody of the evidence from the time of its acquisition from the crime scene until its presentation in court. When you appear at suspect site, you must record the location, the date and time, and the description of all hardware and software subject to investigation, including their descriptions and serial numbers. The Lab also requires the students' demonstration of utilizing the FTK reporting features.

Hiding data – steganography: This topic discusses the history and methods of steganography. In the seventh Lab Exercise, we present the students with files containing several instances of hidden data, and challenge them to find each.

5. LAB INFRASTRUCTURE

To support the lab projects outlined in the previous section, we have developed a plan for a flexible lab infrastructure. The Forensics Laboratory at the University of Alaska Anchorage will be a shared facility, teaching both Digital Forensics classes and general Information Security classes. The lab is designed to easily switch between projects, and to accommodate a variety of possible tasks. A possible list of project types is in (Francia, 2006), many of them along the lines of the outline we presented earlier. The development of the lab infrastructure, policies and will follows the guidelines in (Chen, Tsai, Chen & Yee, 2005) and in (Logan and Clarkson, 2005).

The computers currently in use in the lab are older MicronPC machines that were retired from the main public and classroom labs in the College of Business and Public Policy. These client machines have somewhat limited memory (128-256 MB) and CPU performance (600-800 MHz), but are adequate for running the typical projects anticipated for the lab. All machines have CD-ROM drives, USB ports and fixed hard drives with 15-25 GB of disk space. Image CD's will be used to quickly reconfigure machines with different operating systems and with different configurations settings.

A number of older Compaq servers are also available, with even lower memory and CPU speeds, but with hot swappable hard drives configurable as RAID disk arrays. These machines allow students to install a disk for the duration of the lab session only, and to remove and store the disk for continuing the lab at a later time. This makes for even easier switching between projects. Pending available funding, the plan is to purchase rack mounted machines or newer, higher performance client machines.

The forensics projects includes the standard set of host based forensics and network forensics (Francia, 2006). For host-based projects, students only need to work on one computer, typically a client machine. Students need to acquire a drive and to analyze it. The analysis can include file types, file contents, access statistics from the system logs, client based email forensics, as well as the analysis of web browsing patterns based on the cache contents on the client's disk.

Network Forensics projects involve multiple interconnected client and server machines. Although we have not included such projects in the initial list, we plan to include network forensics labs within the next two years. The computers are already used for teaching Computer Networks, and could easily be adapted for the Network Forensics labs. For precautionary reasons, none of the machines are connected to the campus network or to the Internet. Machines are only connected to each other via hubs and/or routers. The client machines are interconnected using hubs, which makes monitoring the network traffic much more straightforward, because all devices connected to a hub are able to listen to the traffic on the entire network. This is an ideal configuration for exploring Network Forensics projects. Hub connected computers will allow students to experiment with packet sniffing software. Switches will also be used because switches segment traffic into point-to-point connections, students will experiment with MAC address flooding to force switches to also broadcast all the traffic to all of the ports. In addition, the use of routers will expose students to using log files for access lists filtering.

Teaching forensics might also involve the recovery of data from damaged equipment (Gottschalk, Liu, Dathan, Fitzgerald and Stein, 2005). We currently have no plans for specialized equipment, but we will use test cases of equipment in various degrees of damage to demonstrate to students the capabilities and limitations of existing hardware. These labs, along with the Network Forensics labs will be part of a second round of lab curriculum development.

6. COLLABORATION PLAN

In designing and running the Digital Forensics curriculum, the Computer Information Systems Department (CIS) is planning to collaborate with several key local organizations that have a stake in increasing the level of expertise in the state.

The Justice Center at UAA was established in 1975 and serves the teaching (academic and outreach) and research needs in the state. The academic mission includes educating students for legal, law enforcement and correctional careers. Now part of the College of Health, Education, and Social Welfare, the Justice Center was the first of the many research centers organized at UAA in the 1970's. The impetus behind the research component of the Center was the lack of sufficient critical mass in other state agencies in establishing research units of their own. Academic and research interests are tightly coupled in the Center, with undergraduate students involved in many of the research projects, (UAA, n. d.).

We anticipate a close collaboration with faculty from the Justice Center in developing the law enforcement aspects of the curriculum. The sections where Justice Faculty will be involved include those dealing with: Law, investigations, and ethics; Search and seizure issues; Preparation for a forensic investigation; Documenting and reporting the case; and Testifying in court. By working on joint projects with the Justice Center, the Digital Forensics students will be exposed to the law enforcement side of computer crime investigation, while Justice students will have a chance to understand the technological capabilities and limitations.

Another key partner of the Digital Forensics program will be the University Police. The University Police Department's staff consists of professional, full time officers with the same qualifications as any police office in the State of Alaska, but located on campus, and reporting directly to the university administration. The focus of the unit is mainly on non-computer crime, in particular on campus safety and security. The majority of cases investigated by the University Police are larceny and theft, but the CIS Department will collaborate with the UPD on those crimes involving computers or that have investigation components that are computer related.

Outside of the University of Alaska Anchorage, the CIS Department will work with the Anchorage Police Department. In particular, we intend to involve our students in the Ride Along Program, which allows community members to spend an entire shift accompanying a police officer. Currently, this program is open to any community member meeting a basic set of requirements. Participation in the Ride Along Program will enable our students to understand better what the typical law enforcement job entails, as well as to understand how computer and non-computer evidence is acquired in crime cases, (Anchorage Police Department, n. d.).

A second APD program is the Citizen's Academy in which participants attend a ten-week series of classes meeting one night a week. Each night of class consists of two topics. Each topic is taught by police officers, detectives, or other personnel in their fields of expertise which include: Cyber Crime, Fraud/Financial Crime, Homicide Investigations & Evidence Collection, Drug Investigations/Vice Crimes, Emergency Preparedness, Crime Prevention; Child Abuse & Sexual Assault, Tour of the Anchorage Police Department Dispatch & Crime Lab, and other topics, (Anchorage Police Department, n. d.).

The Department will also work closely with several Alaska Native organizations that have an interest in developing digital forensics expertise in the state. Through the Alaska Native Lands Settlement Act (ANCSA) of 1971, Alaska Natives were awarded 11% of the state's area and almost a billion dollars in exchange for land claims elsewhere in the state, in particular in the oil rich areas of the North Slope. The Act also led to the formation of twelve Regional Native Corporations serving shareholders of the respective regions, and a thirteenth "at-large" corporation to sever Natives outside of the Regional Corporations areas. These corporations serve their shareholders both through payment of dividends, as well as through economic development in the regions. Through the 8(a) program, the Federal Government has also granted preferential status to qualifying Native Corporations and subsidiaries. Many of these corporations are involved in research or operations programs and projects for the government including information security and justice in and outside Alaska.

One of the key players that the University of Alaska Anchorage has cooperated with and will continue to cooperate with is Chenega Technology Services Corporation (CTSC). CTSC is associated with the National Law Enforcement and Corrections Technology Center (NLECTC) Northwest as a program of the National Institute of Justice (NIJ). Through our corroboration with them, we have the opportunity to attend a week of hands-on training/working on national security issues at NLECTC Northeast in Rome, N.Y.

The Department is also associated with InfraGard, whose goal is, "to improve and extend information sharing between private industry and the government, particularly the FBI, when it comes to critical national infrastructures.”
"Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. These systems are so vital, that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States." - President William J. Clinton, 1998, (InfraGard, n. d.).

7. CONCLUSIONS

Offering any new course requires careful planning and justification. This is especially true of a Digital Forensics course due to several factors. Setting up a lab to support hands-on assignments is expensive. It is important to have qualified and experienced faculty that have professional investigative experience. It is also important to measure the existing market conditions to determine the need for such a course. We conducted an exploratory study to determine important factors when offering a digital forensics course. We provided the course outline, lab infrastructure, and collaboration plans needed for the design of this course.

The two half-semester pilot DF courses received positive feedback from students. Both law enforcement and local businesses see a need for more Digital Forensics trained professionals. Both the feedback from the students and that from the potential employers were critical factors in our offering a full-semester DF course. We have included feedback obtained from students and prospective employers in the Appendix section. We got feedback from a very small student set because the first half-semester version of the DF course, which was a trial course, was added late to the university class schedule. We have not received the official evaluation sheets for the second half-semester DF course offered in summer 2006; hence, we administered a survey to obtain students’ feedback but got responses from only five students. We have received informal feedback from students interested in taking the full semester DF course after hearing about the course from their peers.

Feedback from law enforcement agencies and prospective employers has also been included in the Appendix. There is a major Information Technology Expo planned for next week in which our department is one of the key participants with a faculty member giving a presentation on Digital Forensics. We plan to gather additional feedback from prospective industry and military employers during this expo.

8. REFERENCES

Anchorage Police Department. Retrieved July 7, 2006, from http://www.muni.org/apd1/apd911.cfm

Badenhausen, K. (2006). Best Places for Business and Career. Retrieved June 5, 2006, from http://www.forbes.com/lists/2006/1/2846.html

Chandler, C. As crimes over the Internet grow, so does your liability. Retrieved June 6, 2006 from http://www.infragard.net/press_room/articles/article_103104.htm

Charter College. Associated Degree Programs. Retrieved July 25, 2006 from http://www.chartercollege.org/pages/associates.htm#security

Chen, P.S., Tsai, L.M.F., Chen, Y.C., & Yee, G. (2005). Standardizing the construction of a digital forensics laboratory, in First International Workshop on Systematic Approaches to Digital Forensic Engineering, November 7-9, 2005.

Federal Bureau of Investigation (FBI). Your Local FBI Office Field Divisions. Retrieved June 25, 2006, from http://www.fbi.gov/contact/fo/fo.htm

Francia, G. (2006). Digital Forensics laboratory Projects, in the Fourth Annual Consortium for Computing in Colleges Mid-South Conference, Memphis, Tennessee 31 March - 1 April 2006.

Gottschalk L., Liu J., Dathan B., Fitzgerald S. and Stein M. (2005). Computer Forensics Programs in Higher Education: A Preliminary Study, in SIGCSE'05, February 23-27, 2005, St. Louis, Missouri, USA.

InfraGard. Retrieved July 7, 2006, from http://www.infragard.net/index.htm

Logan, P and Clarkson, A. (2005). Teaching Students to Hack: Curriculum Issues in Information Security, in SIGCSE'05, February 23-27, 2005, St. Louis, Missouri, USA.

National Security Agency (NSA). NSA and DHS Announce the 2004 Designation of the National Centers of Academic Excellence in Information Assurance Education. Retrieved July 26, 2006 from http://www.nsa.gov/releases/relea00078.cfm

Swartz, J. (2006). Cybercrime spurs college courses in digital forensics Retrieved June 7, 2006, from http://www.usatoday.com/tech/news/techinnovations/2006-06-05-digital-forensics_x.htm?POE=TECISVA

University of Alaska Anchorage Justice Center, Retrieved June 30, 2006, from http://justice.uaa.alaska.edu/jcinfo.html

Wikipedia. Retrieved July 21, 2006 from http://en.wikipedia.org/wiki/Starkville,_Mississippi

Wikipedia. Retrieved September 25, 2006 from http://en.wikipedia.org/wiki/Computer_forensics

APPENDIX

Feedback from Students

Our student feedback is limited because UAA has offered a digital forensics course only twice. The first was a half-semester, experimental course in fall 2005. The second was also a half-semester course presented by Mississippi State University (MSU) faculty in summer 2006.

Feedback received from students who took the first Digital Forensics course

1. What did you like about the course?

- Assignments were fun
- Guest speakers were great
- Sharing of personal experience
- Demonstration of forensic tools
- Lots of valuable Web sites and information
- It was my first time learning about forensics and I really enjoyed it
- The professor made it very interesting

2. What needs to be improved?

- More hands- on practices
- N/A

3. Other comments to make it better.

- More people
- This class should be offered every semester

Feedback received from students who took the second Digital Forensics course taught by MSU faculty

1. How important do you consider Digital Forensics (DF) to be in your career (even if you do not intend to work in that exact area)?

1. This was an amazing look at how digital media is designed and how data can be stored and accessed so it was extremely important.
2. I think it is very important for anyone who works with computers to know. If I became a developer for some company, I think I could help build more secure software with the forensics knowledge that I have.

3. It has made me aware of issues regarding security breeches and what to look for when the UAA system has been breached by hackers (i.e. this spring when student data had been compromised when a hacker penetrated the system, and it makes me aware of my individual area and needs to make my area secure.
4. DF as it relates to data recovery is an essential aspect of most technical fields, especially if you are a sys admin or perform some other related job. In addition, the security aspect of DF is critical no matter what field you are involved in. Every organization that includes technology in its operations must be wary of security concerns.
5. Not so important, but it might come in handy in the future.

2. **Are you looking for a job in DF?**
   - Yes 2
   - No 3

3. **If yes, in what area?**
   - Law enforcement
   - Other

4. **Of the things you learned in the class, which ones would you envision as a career possibility.**
   - Perhaps some contracting in field of Forensics to be an expert witness.
   - If I were to get into this area as a career, I would probably choose to be a private security consultant.
   - Investigation team.
   - I really enjoyed every bit. I really loved the security portion because I am paranoid about security as it is. I also really loved the digital forensics portion of the class because, while it was probably not the most advanced stuff, I felt as if I was doing something that people do on CSI to catch crooks.
   - Computer Forensic career.

5. **Do you expect this class to be useful in your job search after graduation?**
   - Yes 5
   - No 0

6. **Did this course meet your expectations?**
   - Yes 4
   - No 1

7. **If not, why not?**

- I wish that we had more time to learn, because it seems that we have missed a lot of learning skills.

8. Did you feel that you were well prepared for this course?

Yes	4
No	1

9. If not, what prerequisites would have been the most helpful?

- Linux operating systems.

Feedback received from prospective employers in Anchorage

We have listed some comments received from prospective employers below. While none of the comments is a direct quote, the respondents include:

1. Glenn Klinkhart, Anchorage Police Department, Homicide & Cybercrime
2. Mark Huelskoetter, Anchorage Police Department, Cell Phone Forensics
3. Mike Messeck, Conoco-Phillips Security Officer (The three above are also partners in an Anchorage contracting company, DigitalSecurus)
4. Clark Harshbarger, FBI Special Agent

The comments are:

- Computer Security is a science and is similar to the medical profession. It is too broad of a topic for general practitioners. It must have specialists in major areas.
- Our company does not see UAA as a competitor; we view the university as a source of our future employees.
- We will do whatever we can, including speaking at your classes, to help get your security program off the ground.
- We cannot handle all of the requests for assistance that we get, and many companies that need assistance, are not asking for it.
- Corporate America needs more education on digital security; they need to be aware of the magnitude of the potential problems.
- Our society is too eager to embrace new technology. We do not consider the safety factor until after it is too late.