New Graduate Course Proposal

Digital Forensics Applications

Course Title: Digital Forensics Applications

Course description as it is to appear in the catalog:

FCM 7xx. Digital Forensic Applications. Intensive application of computer and network forensics in simulated case work along with critique of actual cases. Includes design of a digital forensics lab, forensic analysis, preparation of case reports, and expert testimony. 2 hours lecture plus laboratory. Prerequisites: CRJ 708, Law Evidence and Ethics, FCM 760, Forensic Management of Digital Evidence, and FCM 742, Network Security, 3 credits.

Prerequisites:

This course is intended to serve as a capstone to the practical side of the program. As such, it has CRJ708 (Law, Evidence and Ethics), FCM760 (Forensic Management of Digital Evidence) and FCM742 (Network Security) as prerequisites.

Rationale for course:

The goal of this course is to provide intensive and supervised application of digital forensic tools through work on simulated criminal cases complemented with discussion of actual cases that have entailed various forensic problems and techniques.

The first rendering of CRJ753 exposed the need to significantly increase the opportunities available for FCM students to apply what they are learning. CRJ753 was designed as a comprehensive survey course that addresses many aspects of electronic crime investigations that would serve both FCM and CRJ students and provide limited experience in working a simulated case involving digital evidence. The demands of serious forensic analysis casework, however, proved to require much more time on the part of students than possible given the charge of CRJ753. Moreover, the level of sophistication necessary to challenge FCM students in practice makes the integration of general CRJ students with FCM students in the same course problematic. Thus a new required applications course is deemed necessary that would allow FCM students to conduct multiple supervised investigations of simulated cases while providing exposure to issues in the field through forensic case studies. Besides practice based on simulated criminal cases, the new course would also cover issues related to expert testimony on those cases, a topic previously not explicitly covered in any FCM course.

The proposed course is intended to experimentally serve as a capstone for the practical side of the program, thus, effectively filling the role that FCM760, Forensic Management of Digital Evidence, had originally been pegged to serve. FCM780 has been reprogrammed to provide a first semester introduction to the field and forensic techniques. Thus we wish to see whether this new temporal structure and this new course, Digital Forensic Applications, will provide an adequate vehicle for to provide students with the applications experience required. If so, Digital Forensic Applications will ultimately replace Investigating Cybercrime (CRJ753) as a required course in the FCM program of study.
Course outline:

NOTE: Lectures are at normally scheduled class time. Lab work is done weekly at a student's convenience.

Week 1  Lecture  The digital forensics toolbox
        Lab     Demonstration Case Study

Week 2  Lecture  First responder/examiner/lab "Best Practices" and standards
        Lab     Case simulation #1

Week 3  Lecture  Rules of evidence and electronic media
        Lab     Case simulation #2

Week 4  Lecture  Imaging and storage
        Lab     Case simulation #3

Week 5  Lecture  Encryption, passwords and steganography
        Lab     Case simulation #4

Week 6  Lecture  Execution of search warrants
        Lab     Case simulation #4 (cont')

Week 7  Lecture  Digital wiretaps and warrants
        Lab     Case simulation #4 (cont')

Week 8  Forensic skills assessment (midterm)

Week 9  Lecture  Keylogging cases
        Lab     Case simulation #5

Week 10 Lecture  Network forensics cases
        Lab     Case simulation #5 (cont')

Week 11 Lecture  Wireless forensics cases
        Lab     Case simulation #6

Week 12 Lecture  Handling multimedia digital devices
        Lab     Case simulation #6 (cont')

Week 13 Lecture  Expert testimony
        Lab     Case simulation #6 (cont')

Week 14 Lecture  Course review
        Lab     Case simulation #6 (cont')

Week 15 Mock testimony/presentation of case findings

Proposed texts and supplementary reading:


USDOJ, (2002). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*


Hosmer, Chet, Digital evidence bag, *Communications of the ACM* Volume 49, Number 2 (2006), Pages 69-70

**Library resources for this course:**

As this course will primarily offer hands practical lab work, library resources appear to be adequate.

**Proposed instructors and qualifications:**

Professor Steve Kim, M.S. (Practicing high technology crime detective, NYPD)

**Other resources needed to offer this course:**

This course will see students use resources available in the Forensic Computing Lab and Classroom. The lab includes such equipment as five professional forensic work stations, a RAID for data storage, a CISCO router and assorted other hardware and software to include EnCase, FTK and Smart. There is need for numerous additional laptops to allow for experimental forensic analysis of networks. At this point, due to a limited number of site licenses for forensic software, students are obliged to use the software on hand in the lab. The college has a site license for the student version of a key product; however, this limited version the software proved inadequate for serious forensic practice. Thus we are seeking a broader site license. Presently, student work in the lab must be done in small groups at various times. Thus more hardware and software are needed to mount this course with optimal effectiveness.

**Possible conflicts with existing courses and programs:** No