Course Outline

A. Course Number and Title: DA205 Digital Forensics II

Prerequisite: Successful completion of DA204.

B. Curriculum: Information Technology (1492), Technical elective

C. Course Description: This course will cover the fundamentals of computer forensics and investigations. Topics will include historical and current computer forensic and investigative security issues; a systematic approach to computer investigations; digital forensics, email and image file analysis; and guidelines for investigation reporting. Various forensic tools will be used during the laboratory portion of the class. Hardware and software issues related to the development of a computer forensics laboratory will be discussed. (N)

D. Duration of Instructional Period: 150 Minutes Lecture
100 Minutes Laboratory
per week for 15 weeks
Four (4) Credit Hours

E. Lecture/Lab/Credit Hours: 3,2,4

F. Suggested Text(s): Guide to Computer Forensics and Investigations
(3rd edition) Nelson/Phillips/Enfinger/ Steuart
Course Technology (http://www.course.com)
0-619-21706-5

G. Course Outcomes:

Upon completion, the student will be able to

1. Utilize a systematic approach to computer investigations.
2. Utilize various forensic tools to collect digital evidence.
3. Perform digital forensics analysis upon Windows, MAC and LINUX operating systems
4. Perform email investigations.
5. Analyze and carve image files both logical and physical
6. Explain guidelines for investigation reporting.
7. Explain anti-forensic methods/tools and their use
8. Understand the implications of anti-forensics to the digital forensics investigator

9. Demonstrate an awareness of current methods of reducing the effectiveness of anti-forensics

H. Program Competencies:
1. Demonstrate technical writing skills
2. Achieve entry-level working knowledge of popular microcomputer application packages.

Certificate Competencies:
Upon completion of the CS&I D/F Certificate, students will:
1. Be able to acquire, validate, extract, analyze and report upon digital evidence.
2. Be conversant with multiple digital devices including, but not limited to: computers, personal digital assistants, cameras, cell phones, ipods, removable flash media.
3. Comprehend the process for digital evidence to be admissible in a court of law.
4. Comprehend the "Chain of Custody" process.
5. Understand the Rules of Evidence, and basic NY State law with regard to the search and seizure of digital evidence.
6. Be knowledgeable about the physical handling of digital devices.
7. Be able to create understandable and accurate reports.

I. SUNY General Education Knowledge and Skills: NA

J. ECC Graduate Learning Outcomes (GLO):
1. Read and think critically (Related Course Objectives 1-8)
2. Exhibit the research skills for lifelong learning. (Related Course Objectives 1-8)
3. Demonstrate adequate preparation for a career or continuing education. (Related Course Objectives 1-8)

K. Assessment of Student Learning:

Assignments	6-10 labs	200 pts
Exams	2	100pts

L. Library Resources: Students are strongly encouraged to use the library and Internet, where appropriate, when completing assignments.

Suggested Resources

Principles and Practice of Information Security
Volonino / Robinson
Prentice Hall (http://www.prenhall.com)
0-13-184027-4

M. Topical Outline:

Topics **Instructional Period**

I. Review of Computer Investigations 1 week

- A. Case examination and assessment
- B. Evidence gathering
- C. Systematic approaches to computer investigations
- D. Conducting an investigation

II. Review Operating and File Systems 1 week

- A. Review of file structures, boot processes, and data structures of popular operating systems.
- B. NTFS
- C. Macintosh
- D. Linux

III. Preparing Media to Accept an Image 1 week

- A. Create a partition
- B. Wipe partition using DOD standard
- C. Verify wipe of partition

IV. Digital Forensics Evidence 2 weeks

- A. Restoring a Hard Disk Image
- B. Verifying restore was successful
- C. Boot to the evidence Operating System

V. Data Acquisition 2 weeks

- A. Identify methods
- B. Utilization of various data acquisition tools

VI. Computer Forensic Analysis 2 weeks

- A. Concepts
- B. Utilization of various analysis tools
- C. Recognizing, locating, recovering and analyzing images
- D. Processing evidence with FTK
- E. Data Carving
- F. Searching the Registry

VII. Linux Forensics 2 weeks

- A. Linux Distributions
- B. Boot block, superblock, inode block and data block
- C. Understanding inodes
- D. Linux Loader & GRUB
- E. Linux drives and partition schemes
- F. Sleuth Kit, Autopsy, HELIX and KNoppix

VIII. MAC Forensics 2 weeks

- A. HFS, HFS+
- B. Finder, File Manager

C. Macintosh acquisition methods using MacQuisition
D. Using Black Bag Tools

IX. Computer Forensic Investigation Reporting 1 week
A. Reporting guidelines

B. Witness Requirements

X. Anti Forensics 1 week
A. Traditional methods
1. Overwriting Data and Metadata
2. <u>Cryptography, Steganography, and other Data Hiding Approaches</u>
3. Decrypting EFS with FTK .
B. Non-traditional methods
1. Targeting forensic tool blind spots
2. Targeting forensic tool vulnerabilities
3. Targeting generic tool/lib vulnerabilities
C. Review of current tools & techniques

N. Prepared by: Donna Marie Kaputa Ph.D.
Louise Kowalski 2008