

# **COURSE OUTLINE**

**CFOR-210**

**Computer Forensics III**

**3 Credits**

## **HOWARD COMMUNITY COLLEGE**

### **Description**

This course covers topics related to advanced concepts in computer forensics and cross validating electronic case data analysis using popular software tools recognized in the computer forensics field. Students will examine electronic communications laws related to PDA's, cell phones and laptop devices. Students will examine how PDA's, cell phones and laptop devices operate, store electronic data, and will become familiar with the major manufacturers of these electronic storage devices. Students will develop basic computer forensic interview techniques and skills. Students will have hands-on laboratory experience using various computer forensic tools and prepare evidence. Prerequisite: CFOR-200. (2 hours lecture, 2 hours lab)

### **Overall Course Objectives**

Upon completion of this course, the student will be able to:

1. Become familiar with the components of the Encase forensic software environment, including the case, evidence and configuration files and how to acquire removable media and validate the image file created.
2. Explore methods of data storage and forensic recovery, specifically the relevant forensic differences between the FAT, NTFS and CD files system, using Access Data Software.
3. Do the cross-validation of computer forensic case data using Encase, Access Data and NTI forensic tools.
4. Compare and contrast the strength and weaknesses of various computer forensic tools discussed in class.
5. Prepare a basic computer forensic hardware and software platform needed to conduct computer forensic analysis in the laboratory.
6. Examine electronic communications laws associated with PDA, cell phones and laptops.
7. Examine the data acquisition procedures for cell phones, PDA and laptops.
8. Describe the operation and electronic storage processes of PDA's, cell phones and laptops.
9. Develop basic computer forensic interviewing techniques and tactics.
10. Research emerging topics related to computer forensics.

### **Major Topics**

- I. Encase Software Familiarization
  - A. Overview of the Encase software interface and basic functions
  - B. Data acquisitions using Encase in the Windows environment
  - C. How Encase searches the evidence file
  - D. Signature analysis using Encase software

- II. Access Data Software Familiarization
  - A. Examine email messages, deleted files, free space and file slack
  - B. Search and export graphic files
  - C. Advanced search and filtering techniques
  
- III. Cross Validation of Electronic Data Files
  - A. Choosing appropriate hardware and software for evidence examination
  - B. Building an appropriate computer forensics hardware and software platform
  - C. Compare and contrast evidence-handling techniques
  
- IV. PDA, Cell Phones and Laptops
  - A. Computer forensic laws
  - B. Computer forensic examination procedures
  - C. Fundamentals of Palm operating system
  - D. Data acquisition using PDA, Cell phones and Laptops
  - E. Wireless technologies
  - F. Use of various data acquisition tools
  
- V. Develop computer forensic interviewing techniques
  - A. Basic interviewing techniques and considerations

### **Course Requirements**

**Grading/exams:** Grading procedures will be determined by the individual faculty member but will be calculated on the basis of tests, lab reports, project and final exam.

**Writing:** Each week, students are expected to write a laboratory report after performing that week's assigned experiments.