

COURSE OUTLINE

CFOR-200

Computer Forensics II

3 Semester Hours

HOWARD COMMUNITY COLLEGE

Description

This course is designed to cover advanced concepts in computer forensic analysis, and the development of investigative thinking and awareness. This course covers basic criminal law concepts, related national electronic laws, and sources of electronic information as it applies to computer forensics. Study of data hiding techniques, encryption and password recovery will also be covered. Students will have hands-on laboratory experience using various computer forensic tools, evidence gathering and documentation techniques.

Prerequisite: CFOR-101. (2 hours lecture, 2 hours lab)

Overall Course Objectives

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

1. Explore various career opportunities for computer forensic examiners.
2. Define identity theft.
3. Define subpoenas and search warrants.
3. Examine local and national laws affecting computer forensic examiners.
4. Identify sources of electronic information for computer forensic examiners.
5. Describe proper evidence handling and seizure techniques using case studies.
6. Prepare electronic evidence documentation reports.
7. Develop investigative thinking and awareness of electronic media.
8. Examine various data hiding techniques.
9. Define encryption terminology and hashing.
10. Compare and contrast electronic password cracking and password recovery tools.

Major Topics

- I. Overview of Computer Forensic
 - A. Career opportunities for computer forensic examiners
 - B. Define identify theft
 - C. Difference between a criminal and civil case

- II. Computer Forensic laws
 - A. Fourth Amendment application to law enforcement
 - B. State of Maryland hacking and electronic access laws
 - C. Familiarization with all national legislative acts related to computer forensics such as the Privacy Act, Anti-Spam Act, Sarbanes-Oxley Act, etc.

- III. Sources of Electronic Information
 - A. Hacking resource sites
 - B. Obtaining domain names/technical contact
 - C. Corporate and Business Information
 - D. Familiarization of DOS Commands

- IV. Evidence Seizure and Documentation
 - A. Definition of evidence
 - B. Subpoena and search warrant

- V. Data Hiding Techniques
 - A. Where and how electronic data is hidden
 - B. Various electronic file formats - jpg, html, gif

- VI. Encryption and Passwords
 - A. Different encryption techniques
 - B. Hashing
 - C. Password cracking tools
 - D. Password recovery

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.