

COURSE OUTLINE
CFOR-120
Computer Forensics Basic Concepts
1 Credit

HOWARD COMMUNITY COLLEGE

Description

This course focuses on the fundamental principles of computer forensics methodology and emerging investigation techniques related to the identification, collection and preservation of digital crime scene evidence. This course emphasizes student awareness in handling suspected digital evidence. (1 hour lecture)

Overall Course Objectives

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

1. Define emerging computer forensics evidence principles and identify the laws related to computer forensics investigations.
2. Describe methods for processing crime and incident scenes and managing the chain of custody for digital evidence.
3. Identify the safety precautions required for working with computer equipment and digital storage devices.
4. Identify basic Personal Computer components, external drives, developing a working familiarity of various types of storage device media.

Major Topics

- I. Defining computer forensics and the role of computer forensic examiner
 - A. Definition of computer forensics
 - B. Role of the First Responder
 - C. Laws related to computer forensics
 - D. Privileged communication and confidentiality
- II. Computer Hardware
 - A. I/O ports
 - B. Memory
 - C. Hard drives, CD-ROM, DVD and external drives
- III. Computer Forensic Tools
 - A. DOS based tools (NTI)
 - B. Encase
 - C. Access data
 - D. Freeware
- IV. File System and File System Management
 - A. Organization of File Systems Basics
 - B. Importance of knowing the file system related to forensic investigations
- V. Digital Evidence seizure, preservation and documentation
 - A. Identification of computers, cables and external devices
 - B. Overview of Handling and Packaging Techniques

Course Requirements

Grading/exams: Grading procedures will be determined by the individual faculty member but will be calculated on the basis of tests, projects and exams.