COURSE OUTLINE
CFOR-101
Computer Forensics I
3 Credits

HOWARD COMMUNITY COLLEGE

Description

This course focuses on the emerging role of the computer forensics examiner, forensic evidence preservation and introduces students to computer forensic tools. This course provides a comparative study of information technology, evidence analysis, chain of custody, and data retrieval from computer hardware and software applications. Students will have hands-on laboratory experience using various computer forensic tools, evidence preservation techniques and documentation. (2 hours lecture, 2 hours lab)

Overall Course Objectives

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

1. Define computer forensics and identify the laws related to computer forensics.
2. Describe processing crime and incident scene and chain of custody.
3. Identify the safety precautions required for working with computer equipment.
4. Identify PC motherboard components such as processor, memory, hard drives, zip drives and overall computer operation.
5. Perform basic forensic examination using DOS operating system.
6. Describe various forensic tools used in computer forensics.
7. Compare and contrast the main features of Windows based operating systems.
8. Install IDE and SCSI hard drives and configure primary partition and logical partition and analyze how data is stored.
9. Apply computer forensic procedures for seizure, preservation and documentation of electronic evidence.
10. Examine the role of unallocated space, RAM slack and file slack in computer forensics.
11. Define privileged communications and confidentiality.

Major Topics

I. Defining computer forensics and the role of computer forensic examiner
   - A. Definition of computer forensics
   - B. Role of computer forensic examiner
   - C. Laws related to computer forensics
   - D. Privileged communication and confidentiality

II. Computer Hardware
   - A. Motherboard
   - B. I/O ports
   - C. Memory
   - D. 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. Various Operating Systems
   A. DOS and DOS commands
   B. Boot process
   C. Configuration files (Registry)

V. File System and File System Management
   A. Organization of File Systems and unallocated file space
   B. Compare and contrast FAT 16, FAT 32 and NTFS
   C. Importance of knowing the file system related to forensic analysis
   D. Examination of electronic evidence using various forensic tools

VI. Evidence seizure preservation and documentation
   A. Install and configure IDE and SCSI hard drives
   B. Primary and logical partitions
   C. Create mirror image

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.