Miami Dade College

Course Description

CIS4366 | Computer Forensics | 4.00 credits

This upper division course, for students majoring in Information Systems Technology, provides the student with knowledge and skills to conduct formal incident investigations. The student will learn how to collect and analyze evidence from Windows and Linux computer systems. Other topics include legal issues, evidence analysis, and report writing. Prerequisite: CIS3360.

Course Competencies:

Competency 1: The student will be able to demonstrate an understanding of computer forensics in today's world by:

1. Defining computer forensics
2. Listing the objectives of computer forensics, including evidence preservation and root cause analysis
3. Describing the types of cyber-crime
4. Discussing legal terms related to computer forensics, including affidavits, case law, chain of custody, e-discovery, and authentication of evidence
5. Discussing legal issues pertaining to computer forensics, including applicable laws and how to testify

Competency 2: The student will be able to maintain an effective digital forensics lab by:

1. Explaining the certification requirements for a computer forensics lab
2. Describing the physical requirements for a computer forensics lab
3. Discussing the criteria for selecting a data recovery workstation
4. Discussing the advantages of using virtual machines for analysis
5. Listing digital forensics software

Competency 3: The student will be able to demonstrate an understanding of the computer investigation process by:

1. Describing the steps in the computer investigation process
2. Investigate a company policy violation
3. Explaining the methodology of investigation
4. Performing case assessment
5. Developing an investigation plan

Competency 4: The student will be able to demonstrate an understanding of first responder procedures by:

1. Defining and illustrating what constitutes potential electronic evidence
2. Describing the role of the first responder
3. Explaining the steps in first responder procedures
4. Avoiding some common mistakes of first responders

Competency 5: The student will be able to demonstrate an understanding of incident handling by:

1. Defining security incidents
2. Explaining the role of CSIRTs
3. Discussing how a CSIRT handles a case
4. Explaining the types of incidents and levels of support

Competency 6: The student will be able to generate an investigative report by:

1. Explaining the need for an investigative report
2. Listing report specifications
3. Describing the layout of an investigative report
4. Discussing the best practices for investigators
5. Performing a detailed evaluation of the evidence to analyze the root cause and implications of the event

Competency 7: The student will be able to perform data acquisition by:

1. Describing various digital evidence storage formats
2. Evaluating various data acquisition methods, including bit-stream imaging
3. Explaining how to validate data acquisitions
4. Using various data acquisition and data validation tools
5. Describing live acquisition methods and tools

Competency 8: The student will be able to demonstrate an understanding of file systems, hard disks, and other devices by:

1. Defining disk drive, hard disks, and hard disk interfaces
2. Examining disk partitions
3. Describing popular Linux file systems
4. Describing the Mac OS X file system
5. Describing Sun Solaris 10 file system and UFS (Unix File System)
6. Describing various Windows file systems, including FAT and NTFS
7. Explaining the EFS recovery key agent
8. Describing CD-ROM and DVD file systems
9. Analyzing hypervisors
10. Discussing data hiding techniques, including using slack space, cryptography, and steganography
11. Using known file filters to identify target data, images, and/or activity efficiently
12. Using various tools (including file carving tools) to recover deleted partitions and files. Using steganography detection tools and cryptanalysis tools
13. Using tools to extract and analyze metadata
14. Performing image file forensics

Competency 9: The student will be able to demonstrate an understanding of the boot process by:

1. Defining boot loader and boot sector
2. Describing the MS-DOS boot process
3. Describing the Windows boot process
4. Describing the Mac OS X boot process
5. Describing the Linux boot process

Competency 10: The student will be able to demonstrate an understanding of Windows forensics by:

1. Collecting volatile and nonvolatile information
2. Performing Windows memory analysis
3. Performing Windows registry analysis
4. Using event logs
5. Identifying other audit events
6. Explaining forensic analysis of event logs
7. Using time analysis tools to perform event correlation
8. Explaining Windows password issues
9. Analyzing data and reconstructing events from Windows systems
10. Using a popular Windows forensic analysis tool

Competency 11: The student will be able to demonstrate an understanding of Linux and Macintosh systems by:

1. Performing data collection using Toolkit
2. Analyzing logs
3. Explaining crash commands
4. Analyzing data and reconstructing events from Linux systems
5. Using Linux forensics tools

Competency 12: The student will be able to crack passwords by:

1. Explaining password terminology

2. Describing various cracking methods, including rainbow tables
3. Explaining system-level password cracking
4. Explaining application software password cracking
5. Using default password databases
6. Using password-cracking tools

Learning Outcomes:

- Solve problems using critical and creative thinking and scientific reasoning
- Demonstrate knowledge of ethical thinking and its application to issues in society
- Use computer and emerging technologies effectively

Updated: Fall 2025