Date Adopted: 2014
Date Reviewed: October 2014
Date Revised: October 2014

CIS 282 Computer Forensics

I. **CIS 282 Computer Forensics – 3 Semester Hours**

II. **Course Description**
This course introduces students to methods of computer forensics and investigations. This course helps prepare students for the International Association of Computer Investigative Specialists (IACIS) certification.

III. **Prerequisite**

IV. **Textbook**
Textbook:
Publisher:
Author:

V. **Course Objectives**

1. Introduction to computer forensics and investigations
2. Recover data from Windows and DOS Systems
3. Describe Macintosh and Linux boot process and disk structures
4. Use various hardware and software tools to perform activities associated with computer forensics
5. Identify and control digital evidence
6. Explain how to acquire digital evidence from disk drives

VI. **General Instructional Objectives**
The **cognitive objective** for this course is for each student to comprehend foundational knowledge of computer forensics and methods of securing forensic evidence.

The **performance objective** of this course will be demonstrated through scenarios.

There are no **affective objectives** directly associated with this course.

VII. **Course Content Outline**

MODULE A – INTRODUCTION TO COMPUTER FORENSICS AND INVESTIGATIONS

- **Understanding computer forensics**
  - Definitions
  - History
  - Computer forensics resources
- Preparing for computing investigations
  - Enforcement agency investigations
  - Corporate investigations
- Maintaining professional conduct

MODULE B – RECOVER DATA FROM WINDOWS AND DOS SYSTEMS

- **File systems**
  - Boot sequence
  - Registry data
  - Disk Drive
- Microsoft file structures
  - Disk partition concerns

  - Boot partition concerns
  - FAT disks
- NTFS disks
  - NTSF system files
  - NTFS attributes
  - NTFS data streams
  - NTFS compressed files
  - NTFS encrypted file systems (EFS)
  - EFS recovery key agents
  - Deleting NTFS files
- Microsoft boot tasks
  - Windows XP, 2000, and NT startup
  - Windows XP system files
- MS-DOS startup tasks
  - Other DOS operating systems

MODULE C – DESCRIBE MACINTOSH AND LINUX BOOT PROCESSES AND DISK STRUCTURES

- **Macintosh file structure**
  - Volumes
- Macintosh boot tasks
- UNIX and Linux disk structures
  - UNIX and Linux overview
  - Inodes
- UNIX and Linux boot processes
  - Linux loader
  - UNIX and Linux drives and partition scheme
- Examining compact disc data structures
  - Other DOS operating systems

MODULE D – COMPUTER FORENSICS TOOLS

- **Evaluating software needs**
  - NIST tools
  - NIJ methods
  - Validating forensics tools
- Command-line forensic tools
  - NTI tools
  - Dx2dump
  - DriveSpy
  - PDWipe
  - Image
  - Part
  - SnapBack DatArrest
  - Byte Back
  - MaresWare
  - DIBS Mycroft v3
- Exploring graphical user interface (GUI) forensics tools
  - AccessData
  - Guidance Software EnCase
  - Ontrack
  - BIAProtect
  - LC Technologies Software
  - WinHex Specialist Edition
  - DIBS Analyzer Professional Forensic Software
  - ProDiscover DFT
  - DataLifter
  - ASRData
  - Internet History Viewer
- Other useful computer forensics tools
  - LTTOOLS

  - Mtools
  - R-Tols
  - Explor2fs
  - @stake
  - TCT and TCTUTILs
  - Ilook
  - HaskKeeper
  - Using Graphic Viewers
- Exploring hardware tools
  - Computing-Investiation Workstations
  - Building a workstation
  - Write-blocker
  - LC Technology International Hardware
  - Forensic computers
  - DIBS
  - Digital Intelligence
  - Image MASSter Solo
  - FastBloc
  - Acard
  - NoWrite
  - Wiebe Tech forensic DirveDock

MODULE E – IDENTIFY AND CONTROL DIGITAL EVIDENCE

- **Identifying digital evidence**
  - Identifying digital evidence
  - Understanding evidence rules
- Securing digital evidence
- Cataloging digital evidence
  - Lab evidence considerations
  - Processing and handling digital evidence
- Storing digital evidence
  - Evidence retention and medial storage needs
  - Documenting evidence
- Obtaining a digital signature

MODULE F – EXPLAIN HOW TO ACQUIRE DIGITAL EVEDIENCE FROM DISK DRIVES

- **Determining methods**
- **Data recovery contingencies**
- MS-DOS acquisition tools
  - DriveSpy
  - Data preservation commands
  - Data manipulation commands
- Windows acquisition tools
- Acquiring data on Linux computers
- Other forensics acquisition tools
  - SnapBack DatArrest
  - SafeBack
  - EnCase

VIII. **Evaluation and Assessment**

Evaluation and assessment will be determined by the instructor and specified on the instructor's class syllabus. Grades will be based upon following scale: A = 90 – 100%, B = 80 – 89%, C = 70 – 79%, D = 60 – 69%, and F = below 60%.

IX. **Attendance**

Students are expected to attend all classes for which they are registered. Students who are unable to attend class regularly, regardless of the reason or circumstance, should withdraw from that class before poor attendance interferes with the student’s ability to achieve the objectives required in the course. Withdrawal from class can affect eligibility for federal financial aid.

X. **Statement on Discrimination/Harassment**

The College and the Alabama State Board of Education are committed to providing both employment and educational environments free of harassment or discrimination related to an individual’s race, color, gender, religion, national origin, age, or disability. Such harassment is a violation of State Board of Education policy. Any practice or behavior that constitutes harassment or discrimination will not be tolerated.

XI. **Americans with Disabilities**

The Rehabilitation Act of 1973 (Section 504) and the Americans with Disabilities Act of 1990 state that qualified students with disabilities who meet the essential functions and academic requirements are entitled to reasonable accommodations. It is the student’s responsibility to provide appropriate disability documentation to the College. The ADA Accommodations Office is in FSC 305 (205-856-7731).