Discipline: Computer Information Systems
Originator: Paul Conrad

RIVERSIDE COMMUNITY COLLEGE DISTRICT
INTEGRATED COURSE OUTLINE OF RECORD

COMPUTER INFORMATION SYSTEMS 27A

CIS-27A : Computer Forensics Fundamentals

College: RIV
Lecture Hours: 54.000
Lab Hours: 18.000
Units: 3.00
Letter Grade

Course Description

Prerequisite: None

Advisory: CIS-27

Course Credit Recommendation: Degree Credit

This course is an introduction to the methods used to properly conduct a computer forensics investigation beginning with a discussion of ethics, while mapping to the objectives of the International Association of Computer Investigative Specialists (IACIS) certification. Topics covered include an overview of computer forensics as a profession; the computer investigation process; understanding operating systems boot processes and disk structures; data acquisition and analysis; technical writing; and a review of familiar computer forensics tools. 54 hours lecture and 18 hours laboratory.

Short Description for Class Schedule

An introduction to the methods used to properly conduct a computer forensics investigation beginning with a discussion of ethics, understanding operating systems boot processes and disk structures, data acquisition and analysis, technical writing, and a review of familiar computer forensics tools.

Entrance Skills:

Before entering the course, students should be able to demonstrate the following skills:

1. **Demonstrate general knowledge of Information Security and Security Standards.**
2. **Demonstrate general knowledge of system audits, monitoring, and recovery.**
3. **Demonstrate general knowledge of software tools.**
4. **Identify general Compliance Laws and Regulations.**

Student Learning Outcomes:

Upon successful completion of the course, students should be able to demonstrate the following skills:

1. **Given specific forensics tools, students will demonstrate the ability to analyze data on a compromised computer disk.**
   - **Critical Thinking:** Students will be able to demonstrate higher-order thinking skills about issues, problems, and explanations for which multiple solutions are possible. Students will be able to explore problems and, where possible, solve them. Students will be able to develop, test, and evaluate rival hypotheses. Students will be able to construct sound arguments and evaluate the arguments of others.
   - **Information Competency & Technology Literacy:** Students will be able to use technology to locate, organize, and evaluate information. They will be able to locate relevant information, judge the reliability of sources, and evaluate the evidence contained in those sources as they construct arguments, make decisions, and solve problems.

2. **Given specific topics to discuss students will be able to explain concepts and terminology used by Computer Forensics Specialists**
   - **Critical Thinking:** Students will be able to demonstrate higher-order thinking skills about issues, problems, and explanations for which multiple solutions are possible. Students will be able to explore problems and, where possible, solve them. Students will be able to develop, test, and evaluate rival hypotheses. Students will be able to construct sound arguments and evaluate the arguments of others.
   - **Information Competency & Technology Literacy:** Students will be able to use technology to locate, organize, and evaluate information. They will be able to locate relevant information, judge

the reliability of sources, and evaluate the evidence contained in those sources as they construct arguments, make decisions, and solve problems.

Course Content:

1. Computer Forensics & Investigations as a Profession
    a. Definition of computer forensics
    b. Preparing for computing investigation
    c. Professional conduct
2. Understanding Computer Investigations
    a. Preparing an investigation
    b. Systematic approach
    c. Data-Recovery workstations and software
3. Working with Windows and DOS Systems
    a. File systems / NTFS Disks
    b. Microsoft file structures / Microsoft boot tasks
4. Macintosh and Linux Boot Processes and Disk Structures
    a. Macintosh file structure / Macintosh Boot task
    b. UNIX and Linux disk structures / UNIX and Linux boot processes
5. The Investigator's Office and Laboratory
    a. Forensic lab certification
    b. Physical layout of the laboratory
    c. Basic forensic workstation
6. Current Tools
    a. Command input/output
    b. Using command-line tools
    c. Graphic User Interface (GUI) tools
    d. Hardware tools
7. Digital Evidence Controls
    a. Identifying digital evidence
    b. Securing digital evidence at an incident scene
    c. Cataloging digital evidence / Storing digital evidence
8. Data Acquisition
    a. Determining best method
    b. Data recovery contingencies
    c. DOS / Windows tools
    d. Linux Computers
9. Computer Forensic Analysis
    a. The process and analysis
    b. DriveSpy / AccessData toolkit
10. E-Mail Investigation
    a. Review of Internet fundamentals
    b. Roles of Client and Server
    c. Crimes and violations
    d. Specialized tools
11. Recovering Image Files
    a. Recognizing an image file / Analyzing image file headers
    b. Data compression
    c. Locating and recovering image files
12. Writing Investigation Reports
    a. Their value
    b. Writing clearly
    c. Formal format

Methods of Instruction:

Methods of instruction used to achieve student learning outcomes may include, but are not limited to, the following activities:

- Class lectures, discussions, or demonstrations will demonstrate the application of computer forensics tools and techinques.
- Quizzes designed to motivate and facilitate the acquisition of concept retention, and serve as a survey of student understanding of topics covered in the course.
- Online and Laboratory assignments to be done through Virtual Machine environments to give the students the opportunity to demonstrate learning of computer forensics tools and techniques.

Methods of Evaluation:

Students will be evaluated for progress in and/or mastery of student learning outcomes using methods of

evaluation which may include, but are not limited to, the following activities:

- Quizzes and examinations designed to measure students' degree of mastery of course objectives of progression toward master of course objectives.
- Exercises and projects designed to demonstrate the acquisition of computer forensics concepts and application skills.
- Oral reports and examinations may be used to measure students' communication, critical thinking, comprehension, and organizational skills.
- Collaborative projects designed to evaluate students' ability to work together to address a given task in the area of computer forensics.
- Computer Laboratory assignments and projects designed to clarify students' individual computer forensics strengths and areas of improvement related to computer forensics tools application skills.
- Common final examination designed to evaluate students' overall achievement of course objectives in computer forensics concepts and forensics tools application skills.

Sample Assignments:

Outside-of-Class Reading Assignments

- The primary assignments for this course involve the application of computer forensics tools and techniques. To support this, students will be assigned textbook reading and/or other resource reading that covers the usage of computer forensic tools and techniques.

Outside-of-Class Writing Assignments

- Writing assignments and exercises that specifically address each learning objective. The writting assignments may be used to improve a student's communication skills.

Other Outside-of-Class Assignments

- Other outside of class assignments for this course involve the application of computer forensics tools and techniques. Utlization of laboratory Virtual Machines set up for applying usage of computer forensics tools and techniques.

Course Materials:

All materials used in this course will be periodically reviewed to ensure that they are appropriate for college level instruction. Possible texts include the following:

Britz, M. T.. *Computer Forensics and Cyber Crime: An Introduction*. 3rd Prentice Hall, 2013.
Nelson, B., Phillips, A.. *Guide to Computer Forensics and Investigation*. 4th Cengage Learning, 2010.

Codes/Dates:

CB05 MOV Transfer Status: N/A (not in college inventory) (D)
CB05 NOR Transfer Status: N/A (not in college inventory) (D)
CB05 RIV Transfer Status: Transfers to CSU Only (B)

Board of Trustees Approval Date: 12/08/2015
COR Rev Date: 12/08/2015