GROSSMONT COLLEGE

Official Course Outline

COMPUTER SCIENCE INFORMATION SYSTEMS 265 – COMPUTER FORENSICS FUNDAMENTALS

1. Course Number Course Title Semester Units Semester Hours

CSIS 265 Computer Forensics 3 2 hours lecture: 32-36 hours

Fundamentals 3 hours lab: 48-54 hours

64-72 outside-of-class hours for lecture

144-162 total hours

2. Course Prerequisites

A “C” grade or higher or “Pass” in CSIS 264 or equivalent

Corequisite

None

Recommended Preparation

None

3. Catalog Description

This course introduces the methods used to properly conduct a computer forensics investigation. Topics include ethics, computer forensics as a profession, the computer investigation process, operating systems boot processes and disk structures, data acquisition and analysis, technical writing, and a review of familiar computer forensics tools.

.

4. Course Objectives

The student will:

a. Describe the features and operation of modern file systems.

b. Perform elementary forensic analysis and data recovery on the FAT (File Allocation Table) systems, using only a hex editor.

c. Evaluate the strengths and weaknesses of various software tools for data recovery.

5. Instructional Facilities

Standard computer lab with one internet-connected workstation per student with appropriate software installed.

6. Special Materials Required of Student

Flash/USB drive or cloud storage for backup of in-class work.

7. Course Content

a. Computer Forensics Investigation Process

b. Searching and Seizing Computers

c. Digital Evidence

d. First Responders Procedures

e. Computer Forensics Lab

f. Hard Disks and File Systems

g. Window Forensics

h. Data Acquisition and Duplication

COMPUTER SCIENCE INFORMATION SYSTEMS 265 – COMPUTER FORENSICS FUNDAMENTALS Page 2

7. Course Content (continued)

i. Recovering Deleted Files and Deleted Partitions

j. Forensics Investigation using Access Data FTK

k. Forensics Investigation Using EnCase

l. Steganography and Image File Forensics

m. Application Password Crackers

n. Log Capturing and Even Correlation

o. Network Forensics, Investigating Logs and Network Traffic

p. Investigate Wireless Attacks

q. Investigate Web Attacks

r. Track Emails and investigating Email Crimes

s. Mobile Forensics

t. Investigative Reports

u. Becoming an Expert Witness

8. Method of Instruction

a. Online computer-based reading assignments

b. Instructor and individual student mentoring

c. Practical application assignments

9. Methods of Evaluating Student Performance

a. Essay examinations with open-ended questions reflecting theoretical and applied situations regarding computer forensics.

b. Laboratory exercises

c. Objective examinations and quizzes including a final exam.

d. Problem solving examination (demonstration of skill applied to a specific scenario)

10. Outside Class Assignments

a. Read the curriculum and assignment instructions

b. Complete assignments such as Netlab and online quizzes

c. Review online resources such as reference materials and videos highlighting current threats.

11. Texts

a. Required Text(s):

Representative example: CHFI Computer Hacking Forensic Investigator Certification All-in-One Exam Guide, [Charles L. Brooks](https://www.mhprofessional.com/catalogsearch/result/?q=Charles%20L.%20Brooks), 2014.

b. Supplementary texts and workbooks:

None.

Addendum: Student Learning Outcomes

Upon successful completion of this course, our students will be able to do the following:

a. Describe different types of digital evidence, rules of evidence, digital evidence examination processes, and electronic crime and digital evidence consideration by crime category.

b. Demonstrate the ability to utilize forensic procedures such as: how to recover deleted files and deleted partitions in Windows, Mac OS X, and Linux.

Date approved by the Governing Board: May 15, 2018