College of San Mateo
Course Outline

☐ New Course
☐ Update/No change
☒ Course Revision (Minor)
☐ Course Revision (Major)

Date: 2/23/07

Department: CIS **Number:** 491

Course Title: Computer Forensics: Search and Seizure **Units:** 3

Hours/Week: **Lecture:** 3 **Lab:** 1 **By Arrangement:** 1

Length of Course

☒ Semester-long
☐ Short course (Number of weeks___)
☐ Open entry/Open exit

Grading

☐ Letter
☐ Credit/No Credit
☒ Grade Option (letter or Credit/No Credit)

1. **Prerequisite** (Attach Enrollment Limitation Validation Form.)

CIS489 or equivalent

2. **Corequisite** (Attach Enrollment Limitation Validation Form.)

None

3. **Recommended Preparation** (Attach Enrollment Validation Form.)

Eligibility for ENGL 838 or 848.

4. **Catalog Description** (Include prerequisites/corequisites/recommended preparation.)

CIS 491 Computer Forensics: Search and Seizure (3.0) (Credit/No Credit or letter grade option.) Three lecture and one lab hour plus one hour by arrangement per week. Prerequisite: CIS 489 or equivalent. Recommended Preparation: eligibility for ENGL 838 or 848. Access to a computer with Internet capability is strongly recommended. Comprehensive course in Computer Forensics Search and Seizure. Includes an overview of computer crime, federal and state guidelines for computer search and seizure, the chain of custody, computer forensics in law enforcement and corporate environments, exercises in digital evidence discovery using forensic hardware and software, special media forensics, documentation, warrants and investigation reports, presentation in court, case studies, and advanced topics such as cryptography, steganography, hostile code, and Internet forensics. May be taken twice for a maximum of 6 units. (CSU)

5. **Class Schedule Description** (Include prerequisites/corequisites/recommended preparation.)

CIS 491 COMPUTER FORENSICS: SEARCH AND SEIZUREComprehensive course in Computer Forensics Search and Seizure. Includes an overview of computer crime, federal and state guidelines for computer search and seizure, the chain of custody, computer forensics in law enforcement and corporate environments, exercises in digital evidence discovery using forensic hardware and software, special media forensics, documentation, warrants and investigation reports, presentation in court, case studies,

and advanced topics such as cryptography, steganography, hostile code, and Internet forensics. Plus one hour by arrangement per week. Prerequisite: CIS 489 or equivalent. Recommended Preparation: eligibility for ENGL 838 or 848. Access to a computer with Internet capability is strongly recommended. May be taken twice for a maximum of 6 units. Credit/No Credit or letter grade option. (CSU)

6. Student Learning Outcomes (Identify 1-6 expected learner outcomes using active verbs.)

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

1. Understand the federal and state legal issues involved in computer search and seizure;
2. Explain how computer forensics is applied by law enforcement and in corporate environments;
3. Discuss the chain of custody-and the discovery of digital evidence using forensic hardware and software;
4. Create and examine the mirror-image of a drive to find specific digital evidence, and document it;
5. Prepare the digital evidence for presentation in court.

7. Course Objectives (Identify specific teaching objectives detailing course content and activities. *For some courses, the course objectives will be the same as the student learning outcomes. If this is the case, please simply indicate this in this section).*

See above

8. Course Content (Brief but complete topical outline of the course that includes major subject areas [1-2 pages]. Should reflect all course objectives listed above. In addition, you may attach a sample course syllabus with a timeline.)

See Topical Outline

9. Representative Instructional Methods (Describe instructor-initiated teaching strategies that will assist students in meeting course objectives. Include examples of out-of-class assignments, required reading and writing assignments, and methods for teaching critical thinking skills.)

The course may include the following instructional methods as determined appropriate by the instructor:
- Lecture will be used to introduce new topics;
- Teacher will model problem-solving techniques;
- Class will solve a simulated computer crime together, each person contributing a potential "next step";
- Students will participate in short in-class projects (in teacher-organized small groups) to ensure that students experiment with the new topics in realistic problem settings;
- Teacher will invite questions AND ANSWERS from students, generating discussion about areas of misunderstanding;
- Teacher will create and manage an Internet conference for discussion of course topics; and
- Students will work in small groups to solve evidence collection assignments.

10. Representative Methods of Evaluation (Describe measurement of student progress toward course objectives. Courses with required writing component and/or problem-solving emphasis must reflect critical thinking component. If skills class, then applied skills.)

- Bi-weekly quizzes (short answer--from textbook material) to provide feedback to students and teacher;
- Assessment of student contributions during class discussion and project time ;
- Individual digital evidence discovery assignments;
- Midterm and Final exams (short answer (textbook material), general problem solving (similar to in-class work), forensic methodology (similar to assignments)) ;

- Assessment of group participation on course projects, including peer-assessment of participation and contribution to the group effort.

11. Representative Text Materials (With few exceptions, texts need to be current. Include publication dates.)

Nelson, Phillips, Enfinger, Stewart, Guide to Computer Forensics and Investigations, Course Technology, 2007
Eoghan Casey, Digital Evidence and Computer Crime, Academic Press, England, 2000.
John Vacca, Computer Forensics Computer Crime Scene Investigation, Charles River Media, Massachusetts, 2002.
Warren Kruse and Jay Heiser, Computer Forensics Incident Response Essentials, Addison-Wesley, Indiana, 2002.

Prepared by: _____
(Signature)

Email address:

Submission Date: _____