College of San Mateo
Official Course Outline

1. **COURSE ID:** CIS 483 **TITLE:** Digital Forensics and Hacking Investigation
   Units: 3.0 units **Hours/Semester:** 48.0-54.0 Lecture hours; and 96.0-108.0 Homework hours
   Method of Grading: Grade Option (Letter Grade or Pass/No Pass)
   Recommended Preparation:
   Eligibility for ENGL 838 or ENGL 848 or ESL 400.
   CIS 110

2. **COURSE DESIGNATION:**
   Degree Credit
   Transfer credit: CSU

3. **COURSE DESCRIPTIONS:**
   Catalog Description:
   This course is an introduction to computer cyber-crime and hacking investigation processes. Topics include computer forensics tools, hacking investigation tools, data recovery, information gathering techniques, computer data preservation techniques, and computer cyber crime investigation techniques. System administrators, security professionals, IT staff, and law enforcement personnel, would benefit from taking this course. Also, this course can help prepare students to pass computer forensics certification examinations, such as the EC-Council Computer Hacking Forensic Investigator (CHFI) or the Certified Forensic Computer Examiner (CFCE) credential.

4. **STUDENT LEARNING OUTCOME(S) (SLO'S):**
   Upon successful completion of this course, a student will meet the following outcomes:
   1. Demonstrate data recovery and cybercrime forensics investigation techniques.
   2. Demonstrate how to collect, seize, and protect evidence
   3. Analyze Windows forensics
   4. Analyze Linux forensics
   5. Analyze Macintosh computer forensics
   6. Perform network analysis
   7. Investigate incident and intrusion response

5. **SPECIFIC INSTRUCTIONAL OBJECTIVES:**
   Upon successful completion of this course, a student will be able to:
   1. Explore the forensics profession
   2. Analyze examples of computer crime
   3. Investigate forensic methods and labs
   4. Learn how to collect, seize, and protect evidence
   5. Examine techniques for hiding and scrambling information
   6. Recover data
   7. Explore e-mail forensics
   8. Analyze Windows forensics
   9. Analyze Linux forensics
   10. Analyze Macintosh computer forensics
   11. Examine mobile forensics
   12. Perform network analysis
   13. Investigate incident and intrusion response
   14. Explore trends and future directions
   15. Explore system forensics resources

6. **COURSE CONTENT:**
   Lecture Content:
   A. Explore the forensics profession
   1. The definition and scope of computer forensics
   2. Understanding the field of digital forensics
   3. Knowledge needed for computer forensics analysis
   4. The Daubert Standard

5. U.S. laws affecting digital forensics
6. Federal guidelines

B. Analyze examples of computer crime

1. How computer crime affects forensics
2. Identity theft
3. Hacking
4. Cyberstalking and harassment
5. Fraud
6. Non-access computer crimes
7. Cyberterrorism

C. Investigate forensic methods and labs

1. Forensic methodologies
2. Formal forensic approaches
3. Documentation of methodologies and findings
4. Evidence handling tasks
5. How to set up a forensic lab
6. Common forensic software programs
7. Forensic certifications

D. Learn how to collect, seize, and protect evidence

1. Proper procedure
2. Handling evidence
3. Storage formats
4. Forensic imaging
5. RAID acquisitions

E. Examine techniques for hiding and scrambling information

1. Steganography
2. Encryption

F. Recover data

1. Undeleting data
2. Recovering information from damaged media

G. Explore e-mail forensics

1. How e-mail works
2. E-mail headers
3. Tracing e-mail
4. E-mail server forensics
5. E-mail and the Law

H. Analyze Windows forensics

1. Windows details
2. Volatile data
3. Windows swap file
4. Windows lobs
5. Windows directories
6. Index.dat
7. The registry

I. Analyze Linux forensics

1. Linux basics
2. Linux file systems
3. Linux logs
4. Linux directories
5. Shell commands for forensics
6. The difficulty of undeleting files in Linux

J. Analyze Macintosh computer forensics

1. Mac basics
2. Macintosh logs
3. Directories
4. Macintosh forensic techniques

K. Examine mobile forensics

1. Cellular device concepts
2. Evidence you can get from a cell phone
3. Seizing evidence from a mobile device

L. Perform network analysis
1. Network packet analysis
2. Network traffic analysis
3. Router forensics
4. Firewall forensics

M. Investigate incident and intrusion response
1. Disaster Recovery
2. Preserving evidence
3. Adding forensics to incident response

N. Explore trends and future directions
1. Technical trends
2. Legal and procedural trends

O. Explore system forensics resources
1. Tools to use
2. Resources
3. Laws

7. **REPRESENTATIVE METHODS OF INSTRUCTION:**

Typical methods of instruction may include:

A. Lecture
B. Lab
C. Activity
D. Directed Study
E. Discussion
F. Experiments
G. Other (Specify): Lecture and visual aids. Discussion of assigned reading. Discussion and problem solving performed in class. Quiz and examination review performed in class. Homework and extended projects.

8. **REPRESENTATIVE ASSIGNMENTS**

Representative assignments in this course may include, but are not limited to the following:

Writing Assignments:

Students will be assigned weekly homework problems from the required textbook. Approximately four extensive analysis projects will be assigned which require problem solving and critical thinking. Students will write a report for each project. Students also will create and deliver presentations.

Reading Assignments:

Students will read all chapters of the required textbook, readings parallel current assignments, and lecture content. Extensive web searching is critical.

Other Outside Assignments:

Weekly homework problems, internet research, and working on presentations.

9. **REPRESENTATIVE METHODS OF EVALUATION**

Representative methods of evaluation may include:

A. Class Participation
B. Class Performance
C. Class Work
D. Exams/Tests
E. Final Class Performance
F. Final Performance
G. Homework
H. Projects
I. Quizzes

J. Research Projects
K. Written examination
L. Final exam and quizzes to evaluate comprehension and mastery of key terms and concepts as well as application skills related to analysis and synthesis of computer concepts. Participation in lab skills exercises that demonstrate the ability to critically evaluate the proper use of appropriate computer security software to complete a given set of computer -related tasks.

10. **REPRESENTATIVE TEXT(S):**
Possible textbooks include:
A. Easttom, Chuck.. *System Forensics, Investigations and Response,* second ed. Jones and Bartlett Learning LLC, an Ascent Learning Company, 2014

Origination Date: March 2017
Curriculum Committee Approval Date: September 2018
Effective Term: Fall 2019
Course Originator: Kamran Eftekhari