Course ID: CIMS 140
Cat ID: 992300.00
State ID: CCC000521377

College:	A	Saddleback College
Division/School:	BS	Business Science
Department:	CIM	Computer Information Management
Program:	CIMNAD	Network Administrator
Subject:	CIMNAD	Network Administrator

O F F I C I A L C O U R S E O U T L I N E

HISTORY AND STATUS

Course Status: A Active (Fully Approved)
Course Originator: Steve Korper

Board of Trustees	08/26/19
State Approval	02/22/10
Curriculum Committee Approval	08/01/19
Division Approval	08/01/19
Tech Review Approval	08/01/19

Technical Change Date:

Technical Change Comment:
2/25/13-fr CIM 293 to CIMS 240

Comments:
nc fr ST 450017.00

BRIEF DESCRIPTION

Short Title: COMPUTER FORENSICS
Full Title: INTRODUCTION TO COMPUTER FORENSICS

BRIEF DESCRIPTION

Catalog Description:

Students learn skills to launch and properly complete a successful 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; setting up a forensics lab; and a review of familiar computer forensics tools. Features free downloads of the latest forensic software, so students can become familiar with the tools of the trade.

Prerequisite:

None

Enrollment Limitation:

None

Corequisite:

None

Recommended Preparation:

None

COURSE FUNCTIONS

Course Prior to:	Y	Not Applicable
Course Classification:	Y	Credit Course
SC/IVC GE Code:	NA - Not Applicable	
CSU GE Code:	NA	Not Applicable
IGETC GE Code:	NA - Not Applicable	
UC Transferable Course:	N	No UC credit
Comparable SC/IVC:		
Comparable CSU:	CSU CSU San Bernardino IST 275 - Information Networking and Security	
Comparable UC:		
Comparable CCC Baccalaureate:		
TOP Code:	0708.10	Network Administrator
SAM Code:	D	Possibly Occupational
CAN Number:		
CID Number:		

COURSE OPTIONS

Grading Option:	GR	Letter Grade or Pass/No Pass
Open Entry:	N	No
Fixed, Optional or Variable Units:	F	Fixed Units
Repeatability Status:	N	No
Repeatability Model:		
Repeatability Limit:	0	
Cross-Listed Courses:	NONE	
Cross-Listed Parent:	No	

COURSE VALUES

Method of Instruction:	L-L	Lecture/Lab Combination	
Maximum Enrollment:	30	Maximum WSCH:	150
Average Enrollment:	22	Average WSCH:	110

	Lecture	Lab	Learn Ctr	Total
WFCH	2.00	3.00	0.00	5.00
TFCH	33.20	49.80	0.00	83.00
TSCH	33.20	49.80	0.00	83.00
LHE	2.00	2.50	0.00	4.50
FTEF	13.33	16.67	0.00	30.00
UNITS	2.00	1.00	0.00	3.00

Schedule Description:

Students launch and properly complete a successful computer forensics investigation beginning with a discussion of ethics, while mapping to the objectives of the IACIS certification. Guides students through conducting a high-tech investigation, from acquiring digital evidence to reporting its findings. (Formerly CIMS 240).

COURSE CONTENT
(Topics Covered)

Lecture Topics:

I. Computer Forensics as a profession
II. Computing Investigation Processes
III. Microsoft operating systems, boot processes and disk structures
IV. Macintosh and Linux boot processes and file systems
V. The Investigator's Office and Laboratory
VI. Current Computer Forensics Tools
VII. Digital evidence controls.
VIII. Processing Crime and Incident Scenes
IX. Data acquisition
X. Computer Forensics Analysis
XI. Email Investigations
XII. Recovering Graphics Files
XIII. Expert Testimony in High-Tech Investigations
XIV. Virtual Machines, Network Forensics, and Live Acquisitions
XV. Cell Phone and Mobile Device Forensics
XVI. Report Writing for High-Tech Investigations

Lab/Learning Center Content:

I. Labs on how data is stored and managed by an operating system.
II. Hands-on labs on email analysis and investigation
III. Hands-on exercises on using current computer forensics tools
IV. Hands-on exercises on data acquisition and graphic image recovery
V. Hands-on labs on generating reports
VI. Hands-on labs on both the Windows and Linux operating system boot process.

COURSE CONTENT
(Learning Objectives)

Students participating in this class will:

1. Define and describe computer forensics technology
2. Summarize how to prepare for a computer investigation
3. Summarize the certification requirements for computer forensics labs.
4. Collect evidence, seize data and measure different ways for proper data acquistion
5. Inspect computer forensics evidence, capture and classify the rules for proper digital evidence handling.
6. Analyze how data is stored and managed by an operating system.
7. Analyze various computer forensics tools and research types of computer forensics systems.
8. Validate the evidence during the analysis process.
9. Identify and reconstruct graphic files and past events.
10. Describe the importance of network forensics.
11. Analyze email investigations.
12. Generate a forensics report.
13. Describe guidelines for testifying in court.
14. Discuss how to maintain a high level of ethical behaviour in your work.
15. Review the anatomy of a hard drive
16. Manage the duplication and preservation of digital evidence
17. Perform computer image verification and authentication
18. Perform the discovery of electronic evidence

COURSE CONTENT
(Student Learning Outcomes)

Students completing this course satisfactorily will be able to:

1. Apply knowledge of computers, software, the law, and investigative techniques to research a possible criminal or civil infraction.
2. Define a method for conducting the analysis of computer and/or network equipment, and related data files.
3. Describe the dynamics of “white collar crime” and identify methods used by white-collar criminals.

COURSE CONTENT
(Methods of Evaluation)

Evaluation of the student will be based upon the following items:

1. Writing Assignments
   short answers
   other (specify)
   a. Students will be evaluated on out of class writing assignments that test for comparisons, recognition and evaluations of course topics.

2. Problem Solving Demonstrations
   quizzes

other (specify)
a. Students will be evaluated on their performance on objective and subjective examinations that test for definitions, recognition and evaluation of topics.

3. Skill Demonstrations
class performance(s)
performance (exam)
other (specify)
a. Students will be evaluated on their computer forensics analysis with disk imaging, data recovery, and data analysis.
Oral presentations and class discussion that test for problem solving, criticism, organization and appraisal of the following topics: Examine and discuss the nature of Computer Forensic Investigations-past, present, and future trends; various cyber crimes; computer language formats; hard drive anatomy; memory allocation; data hiding techniques; data retrieval tools and procedures; retrieved data interpretation; disk imaging software and procedures; network forensic analysis; analysis of various crime examples.

4. Examinations
multiple choice, true/false
other (specify)
a. Students will be evaluated on objective and subjective examinations that test for definitions, recognition and evaluation of topics.

5. Other
other (specify)
a.
Evaluation will include hands-on projects as much as possible.

COURSE CONTENT
(In and Out-of-Class Assignments)

1. Typical Reading Assignments:
   College-level text.

2. Typical Writing Assignments:
   Definitions of the terminology related to computer forensics.

3. Typical Oral Assignments:
   Brief presentation describing evidence found during investigation.

COURSE CONTENT
(Other Requirements)

Textbooks / Supplies:
Nelson, Guide to Computer Forensics and Investigations, 5th Ed. Course Technology. 2016
Britz, M. T., Computer Forensics and Cyber Crime: An Introduction, 3rd Ed. Pearson. 2013
Nelson, B. & Phillips, A, Guide to Computer Forensics and Investigations (MindTap Course List), 6th Ed. Cengage Learning. 2018

Material Fees: $ 0.00 Transaction Code:

VALIDATION
(Corequisite, Limitation on Enrollment,
Prerequisite and Recommended Preparation)