CIS 065: COMPUTER FORENSICS FUNDAMENTALS

Originator
maflores

Co-Contributor(s)

Name(s)
Marhuenda-Donate, Felix

Justification / Rationale
A. This course is being created to conform with the new requirements for the apprenticeship program

Effective Term
Fall 2022

Credit Status
Credit - Degree Applicable

Subject
CIS - Computer Information Systems

Course Number
065

Full Course Title
Computer Forensics Fundamentals

Short Title
COMPUTER FORENSICS

Discipline

Disciplines List
Computer Information Systems (Computer network installation, microcomputer technology, computer applications)

Modality
Face-to-Face
100% Online
Hybrid

Catalog Description
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.

Schedule Description
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. Prerequisite: CIS 060

Lecture Units
2

Lecture Semester Hours
36

Lab Units
1

Lab Semester Hours
54

In-class Hours
90

Out-of-class Hours
72

Total Course Units
3

Total Semester Hours
162

Prerequisite Course(s)
CIS 060 or equivalent

Required Text and Other Instructional Materials

Resource Type
Book (Recommended)

Author
Nelson, B., Phillips, A., Christopher Steuart

Title
Guide to Computer Forensics and Investigations, Cengage

Edition
6th

Publisher
Cengage Learning Inc

Year
2021

Resource Type
Book

Author
Bill Nelson, Amelia Phillips, Christopher Steuart

Title
Guide to Computer Forensics and Investigations

Edition
6th

Publisher
Cengage

Year
2019

College Level
Yes

ISBN #
978-1-337-56894-4

Class Size Maximum
35

Requisite Course Objectives
CIS 060-Describe the fundamental principles of information systems security.

Requisite Course Objectives
CIS 060-Define the concepts of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related.

Requisite Course Objectives
CIS 060-Evaluate the need for the careful design of a secure organizational information infrastructure.

Requisite Course Objectives
CIS 060-Perform risk analysis and risk management.

Requisite Course Objectives
CIS 060-Determine both technical and administrative mitigation approaches.

Requisite Course Objectives
CIS 060-Create and maintain a comprehensive security model.

Requisite Course Objectives
CIS 060-Design and guide the development of an organization’s security policy.

Requisite Course Objectives
CIS 060-Determine appropriate strategies to assure confidentiality, integrity, and availability of information.

Requisite Course Objectives
CIS 060-Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/ controls.

Requisite Course Objectives
CIS 060-Explain the need for a comprehensive security model and its implications for the security manager or Chief Security Officer (CSO).

Course Content
1. Computer Forensics as a profession
2. Computing investigation processes
3. Microsoft operating systems, boot processes, and disk structures
4. Macintosh and Linux operating systems, boot processes, and disk structures
5. The investigator’s office
6. Current computer forensics tools
7. Digital evidence controls
8. Crime/incident scene processing
9. Data acquisition
10. Computing forensics analysis
11. Email investigations

12. Graphic image recovery
13. High tech reports
14. Expert witness overview

Lab Content

1. Understanding the Digital Forensics Profession and Investigations
2. Data Acquisition
3. Processing Crime and Incident Scenes
4. Working with Windows and CLI Systems
5. Current Digital Forensics
6. Linux File Systems
7. Recovering Graphics Files
8. Digital Forensics Analysis and Validation
9. Virtual Machine Forensics, Live Acquisitions, and Network Forensics
10. Email and Social Media Investigations
11. Mobile Device Forensics
12. Cloud Forensics
13. Report Writing for High-Tech Investigations

Course Objectives

	Objectives
Objective 1	Define computer forensics.
Objective 2	Summarize how to prepare for a computer investigation.
Objective 3	Measure the different ways for proper data acquisition.
Objective 4	Classify the rules for proper digital evidence handling.
Objective 5	Classify the rules for proper digital evidence handling.
Objective 6	Analyze how data is stored and managed by an operating system.
Objective 7	Analyze various computer forensics tools.
Objective 8	Validate the evidence during the analysis process.
Objective 9	Identify and reconstruct graphics files.
Objective 10	Describe the importance of network forensics.
Objective 11	Analyze email investigations.
Objective 12	Generate a forensic report.
Objective 13	Describe guidelines for testifying in court.
Objective 14	Maintain a high level of ethical behavior in their work.

Student Learning Outcomes

	Upon satisfactory completion of this course, students will be able to:
Outcome 1	Explain the difference between scientific conclusions and legal decision-making
Outcome 2	Explain the role of digital forensics and the relationship of digital forensics to traditional forensic science, traditional science, and the appropriate use of scientific methods
Outcome 3	Outline a range of situations where digital forensics may be applicable

Methods of Instruction

Method	Please provide a description or examples of how each instructional method will be used in this course.
Discussion	Weekly discussion topics on hacking case analysis.
Collaborative/Team	Students will work in groups to determine possible forensic procedures.
Activity	Attempt to secure a computer as evidence
Technology-based instruction	Utilize simulations and other IT equipment.

Participation	Students will be engaged with daily classroom or online forum participation.
Observation	Watch the Instructor demonstrate computer forensic techniques
Laboratory	Continuing work throughout the course using hands-on (classroom) and virtual computing devices and software.
Lecture	Attend Instructor Lectures

Methods of Evaluation

Method	Please provide a description or examples of how each evaluation method will be used in this course.	Type of Assignment
Written homework	Written online assignments with topics relevant to the curriculum.	In and Out of Class
Student participation/contribution	Students will describe to the class steps taken to troubleshoot issues.	In and Out of Class
Tests/Quizzes/Examinations	Testing of each learning module.	In and Out of Class
Group activity participation/observation	Class and individual projects such as securing a computer for evidence	In and Out of Class
Presentations/student demonstration observations	Hands-on-projects and a combination of examinations, presentations, discussions, or problem-solving assignments. Presentations of projects within specific modules.	In and Out of Class
Computational/problem-solving evaluations	Solve the labs dealing with computer forensics	In and Out of Class
Laboratory projects	Laboratory projects/performance using Encase or Forensic Tool Kit	In and Out of Class
Mid-term and final evaluations	Final examination/skills assessment in industry-recognized security certification	In and Out of Class

Assignments

Other In-class Assignments

1. What are the four basic steps to computer forensics?
2. What are the three (3) C's:
3. What are the Different branches in Digital Forensics
4. What are the 5 different phases of digital devices in Forensics?

Other Out-of-class Assignments

Case Study 1, BTK
In 2005, serial killer Dennis Rader, also known as BTK, was arrested and convicted of murdering 10people in Kansas between the years of 1974 and 1991. Further research this incident using quality and reputable resources.

Write a two to three (2-3) page paper in which you:
1. Explicate how digital forensics was used to identify Rader as a suspect and lead to more concrete physical evidence.
2. Describe in detail the digital evidence that was uncovered from the floppy disk obtained from Rader. Discuss why you believe it took so many years to find concrete evidence in order to build a case against Rader.
3. Explain how the acquisition of digital evidence aided the investigation and whether or not you believe Rader would've been a person of interest if the floppy disk evidence wasn't sent.

Forensic Lab Design
Imagine the university that employs you as an information security professional has recently identified the need to design and build a digital forensic laboratory. You have been tasked with designing the lab for the organization.
Write a four to five (4-5) page paper in which you:
1. Explicate the steps you would take to plan a budget for the lab, keeping in mind the general business objective to avoid unneeded costs.
2. Recommend the physical requirements and controls that you would consider implementing in order to keep the lab safe and secure.
3. Identify at least three (3) hardware and software tools that you would include in the design of the lab and explain your reasons behind your choices.
4. Identify the high-level criteria that would be considered when selecting the forensic workstations to be utilized.

External Intrusion of the PlayStation Network
On April 20, 2011, the Sony PlayStation Network was taken offline after an external intrusion was discovered. Further research this incident using quality and reputable resources.

Write a two to three (2-3) page paper in which you:
1. Briefly summarize the details of the attack on the PlayStation Network, including the dates of when the attack started and was eventually uncovered.
2. Indicate what explanation Sony officials gave for the length of time that had passed from the start of the attack to when the general public was made aware of the details.
3. Analyze and explain what you believe the correct forensic investigative action would have been once the attack was uncovered

Securing the Scene
Imagine you are a digital forensic investigator for a healthcare organization. You learn from your internal information security department that an employee has been using password-cracking software to access confidential customer insurance information. The account information extracted is unknown at this time, though it appears as though multiple computers were being used for the crime and it isn't clear whether an attack is currently in progress. The employee has been detained but his computers remain online.
Write a two to three (2-3) page paper in which you:
1. Develop a detailed plan to approach and secure the incident scene based on the information you have from the scenario.
2. Discuss the initial steps you would take for the investigation, depending on whether or not the attack is still in progress. Include how your actions would differ based on the current status of the incident.
3. Explicate the importance of creating an order of volatility by identifying the potential evidence that is the most volatile. Explain, in detail, how you would extract this evidence.

Casey Anthony Trial
On July 5, 2011, Casey Anthony was found not guilty of first-degree murder in the 2008 death of her daughter, Caylee. Further research this incident using quality and reputable resources.
Write a two to three (2-3) page paper in which you:
1. Provide a brief summary of the background, charges, and trial of this high-profile court case.
2. Explain, from a forensics perspective, the digital evidence found on the Anthony family computer that helped the prosecutors build a case against Anthony.
3. Describe what the prosecution was unable to prove based on the digital evidence found. Indicate whether or not you think this is a common problem with digital evidence and provide a rationale for your response.
4. Explain the software issue that was found to have caused inaccurate evidence to be admitted into the trial.

Data-Hiding Techniques
Suppose you are the Chief Security Officer for a financial institution. Someone on your information security staff has informed you that recent Web content filters have shown an end-user who has been visiting sites dedicated to the alternate data stream (ADS) and steganography hiding techniques. She is interested in what the end-user may be doing and comes to you for some explanation on these techniques. Write a two to three (2-3) page paper in which you:

1. Explain how a user could utilize ADS to hide data and explain other destructive uses which exist for ADS.

2. Determine how rootkits can be used as an alternative for data hiding and explicate why they can be used for this purpose.

3. Describe the processes and tools used by an investigator in determining whether signs of steganography are present in a given situation.

Investigating Data Theft
Suppose a large aerospace engineering firm has immediately hired you as a consultant to investigate a potential violation of corporate policy and data theft. You have been informed that an employee may have been using corporate email to send confidential corporate information to one or more personal email accounts, which may or may not belong to him. You have been told that this action has been happening each business day for the last 13 days and the employee is unaware of any suspicion.

Write an eight to ten (8-10) page paper in which you:
1. Explain, in detail, the initial actions you would take based on the provided information including formal plans to preserve the crime scene(s) and eventual transportation of evidence to a lab.
2. Analyze the physical and logical places where you would look for potential evidence on the suspects computer(s) and / or network servers.
3. Describe, in detail, how you proceed with the email investigation, including the review of email headers and tracing.
4. Describe the processes that would be utilized in order to recover data that may have been deleted from the suspect's computer(s).

Grade Methods

Letter Grade Only

Distance Education Checklist

Include the percentage of online and on-campus instruction you anticipate.

Online %

100

On-campus %

100

What will you be doing in the face-to-face sections of your course that necessitates a hybrid delivery vs a fully online delivery?
We will be using materials provided by the publisher and others that professionals use in the industry. We will maintain proper vigilance to ensure our materials are relevant, cost-effective, and appropriate for online instruction.

Lab Courses

How will the lab component of your course be differentiated from the lecture component of the course?
Labs will be hands-on training using specific applications, software, and equipment to complete a certain task

From the COR list, what activities are specified as lab, and how will those be monitored by the instructor?
The labs are monitored by the instructor using a scoring system and annotated in the grade book

How will you assess the online delivery of lab activities?
The labs are online in the MindTap servers

Instructional Materials and Resources

If you use any other technologies in addition to the college LMS, what other technologies will you use and how are you ensuring student data security?
We rely on our partners to provide such security to their systems to protect our students' data. Our data, on the other hand, is secured through Canvas.

If used, explain how specific materials and resources outside the LMS will be used to enhance student learning.
Labs and courseware are fully online except for some labs performed in a face to face class

Effective Student/Faculty Contact

Which of the following methods of regular, timely, and effective student/faculty contact will be used in this course?

Within Course Management System:
Chat room/instant messaging
Discussion forums with substantive instructor participation
Online quizzes and examinations
Private messages
Regular virtual office hours
Timely feedback and return of student work as specified in the syllabus
Weekly announcements

External to Course Management System:
Direct e-mail
Posted audio/video (including YouTube, 3cmediasolutions, etc.)
Synchronous audio/video
Teleconferencing
Telephone contact/voicemail

For hybrid courses:
Orientation, study, and/or review sessions
Scheduled Face-to-Face group or individual meetings
Supplemental seminar or study sessions

Briefly discuss how the selected strategies above will be used to maintain Regular Effective Contact in the course.
There will be weekly discussions regarding topics related to the course with appropriate instructor participation.
Students will create logs describing the process to diagnose an issue. These logs are uploaded to the LMS and receive appropriate instructor feedback.

If interacting with students outside the LMS, explain how additional interactions with students outside the LMS will enhance student learning.
We have researched various approaches to teaching this course and have compiled them into this course. We have strongly considered the fact that this course may have to be taught online primarily considering the current situation.
Other Information

Other Information

Comparable Transfer Course Information

University System
CSU

Campus
CSU San Bernardino

Course Number
5250

Course Title
Incident Handling and Cyber

Catalog Year
2021

MIS Course Data

CIP Code
11.0101 - Computer and Information Sciences, General.

TOP Code
070100 - Information Technology, General

SAM Code
C - Clearly Occupational

Basic Skills Status
Not Basic Skills

Prior College Level
Not applicable

Cooperative Work Experience
Not a Coop Course

Course Classification Status
Credit Course

Approved Special Class
Not special class

Noncredit Category
Not Applicable, Credit Course

Funding Agency Category
Not Applicable

Program Status
Program Applicable

Transfer Status
Transferable to CSU only

General Education Status
Y = Not applicable

Support Course Status
N = Course is not a support course

Allow Audit
No

Repeatability
No

Materials Fee
No

Additional Fees?
No

Approvals

Curriculum Committee Approval Date
04/05/2022

Academic Senate Approval Date
04/28/2022

Board of Trustees Approval Date
06/16/2022

Chancellor's Office Approval Date
06/18/2022

Course Control Number
CCC000632408