IT 0165 - COMPUTER FORENSICS FUNDAMENTALS

Catalog Description

Formerly known as CIS 88
Also known as ADMJ 88
Advisory: Completion of ADMJ 54 and IT 120 with grades of "C" or better
Hours: 72 (54 lecture, 18 laboratory)
Description: Introduction to the methods used to properly conduct a computer forensics investigation, beginning with a discussion of ethics, while mapping 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. (C-ID ITIS 165) (CSU)

Course Student Learning Outcomes

- CSLO #1: Research, analyze and evaluate information to solve business problems using appropriate computer forensic technology.
- CSLO #2: Design and produce data computer forensic solutions incorporating current trends, security, and best practices.
- CSLO #3: Employ computer forensic concepts and terminology in professional communication.
- CSLO #4: Demonstrate marketable computer forensic career skills.

Effective Term

Fall 2020

Course Type

Credit - Degree-applicable

Contact Hours

72

Outside of Class Hours

108

Total Student Learning Hours

180

Course Objectives

Lecture:
1. Identify the available career paths associated with computer forensics professionals.
2. Detail the processes associated with computer forensics investigations, including initial investigative steps involved in a systematic approach that involves assessment, planning, securing evidence, copying evidence, and evidence analysis.
3. Provide a description of the specific needs of a forensics laboratory, including environmental conditions, communications needs, evidence security, auditing, facility equipment, software requirements, forensic workstation requirements, and the maintenance of operating systems and software.
4. Describe the available computer forensics tools (software), including the strengths and weaknesses of each and where they best serve the needs of a forensics examiner.
5. Explain processes associated with the control of digital evidence, including the maintenance of "chain of custody."
6. Detail specific aspects of email investigation, including policies relating to privacy issues, identity of source and destination, and recovery of erased emails.
7. Describe available forensics resources available for the analysis of network data traffic.
Laboratory:
1. Utilize a specific commercial computer forensics software; display a proficiency in mastering the product's ability to recover erased data.
2. Demonstrate effective writing skills designed to meet the objectives of creating an investigative report.
3. Demonstrate the use of computer forensics software to analyze a network traffic and prepare a brief that outlines what possible problems were found.

General Education Information

- Approved College Associate Degree GE Applicability
- CSU GE Applicability (Recommended-requires CSU approval)
- Cal-GETC Applicability (Recommended - Requires External Approval)
- IGETC Applicability (Recommended-requires CSU/UC approval)

Articulation Information

- CSU Transferable

Methods of Evaluation

- Objective Examinations
  - Example: Instructor will prepare multiple, true/false and fill-in choice questions. Example: True/False - The following are proper steps to take for collecting and evaluating digital content for an investigation: 1) Obtain authorization to search and seize. 2) Secure the area, which may be a crime scene. 3) Document the chain of custody of every item that was seized. 4) Bag, tag, and safely transport the equipment and e-evidence. 5) Acquire the e-evidence from the equipment by using forensically sound methods and tools to create a forensic image of the e-evidence. 6) Keep the original material in a safe, secured location. 7) Design your review strategy of the e-evidence, including lists of keywords and search terms
- Problem Solving Examinations
  - Example: Students will be given scenario based question describing a problem and the parameters involved and asked to determine the proper course of action that needs to be taken to correct the problem. Example: The network administrator has indicated that unusual traffic is passing through the Firewall to and from a particular website that should not be accessed from company computers. A network traffic capture was done using Wireshark. You have been asked to examine the captured traffic and determine which computer the traffic was originating from. Using the saved Wireshark network traffic sample analyze the captured packets and identify suspect traffic as it relates to the investigation.
- Projects
  - Example: Students will be tasked with providing written instructions on how to complete a specific search function in evidence collection software. Their written instructions will be

evaluated based upon both clarity and the ease with which a novice user could follow the instructions with special attention given to the utilization of screen shots to help users navigate through the exercise.

- Skill Demonstrations
  - Example: Students are required to complete a variety of hands-on labs such as demonstrating their ability to discover hidden digital photographs located in the "slack area" of a computer's hard drive within a pre-determined time frame. Students shall show task completion by describing file details including size and date of creation.

Repeatable

No

Methods of Instruction

- Laboratory
- Lecture/Discussion
- Distance Learning

Lab:

1. Through a demonstration by instructor on two different software tools designed to locate missing and deleted files, students will be asked to locate similar deleted files on a hard drive image, demonstrating proper utilization of their chosen software product. Students shall show task completion by describing file details including file name, file size, and file date of creation. Students shall repeat the process utilizing the other software product, searching for an entirely different group of files and asked to provide the same proof of discovery (file name, size, date of creation). Students will prepare a written report of their findings which will be graded using a rubric provided.

Lecture:

1. Students will use Internet research to identify key differences between the two versions of forensic software. During class, the instructor will lead a discussion to evaluate and rate key differences, with the class arriving at a rating consensus as to what are important and less important differences.

Distance Learning

1. The LMS can be used to initiate discussion between the instructor and students, as well as, student to student similar to those that would take place in an on-ground course. With the help of students, the instructor shall develop a crime scene scenario, with students providing input as to the scene, including hardware and computer software that is present. Once the scenario is completed, students shall identify, as a small group exercise, what sort of forensics equipment should be brought to the crime scene and how it will be utilized. Groups shall share their list of equipment with the other groups as a comparison exercise.

Typical Out of Class Assignments

Reading Assignments

1. Read Chapter 3 in your book and be ready to discuss the specific layout you would have for a home office that would serve as your investigations laboratory. 2. Read section of Chapter 5 of your book relating to "Understanding Concepts and Terms Used in Warrants," and be able to discuss the "plain view doctrine" in class.

Writing, Problem Solving or Performance

1. Research any two computer forensics products on the Internet, and prepare a five (5) page written report comparing and contrasting the products, identifying key features and product shortcomings. 2. Search the Internet for a current news article that described a criminal activity involving computers and write a two (2) page report, indicating your thoughts on how this activity could have been prevented.

Other (Term projects, research papers, portfolios, etc.)

Required Materials

- Guide to Computer Forensics and Investigations
  - Author: Bill Nelson
  - Publisher: Cengage Learning
  - Publication Date: 2019
  - Text Edition: 6th
  - Classic Textbook?: No
  - OER Link:
  - OER:

Other materials and-or supplies required of students that contribute to the cost of the course.