Course Acronym:	CIS
Course Number:	120
Descriptive Title:	Digital Forensics
Division:	Business
Department:	Computer Information Systems
Course Disciplines:	Computer Information Systems
Catalog Description:	This course introduces students to digital forensics, focusing on evidence found in computers and digital media. Topics include the analysis of digital evidence, chain of custody, forensic tools, and recognizing compromised systems. Students will learn the proper techniques used to investigate a security breach as well as how to analyze and preserve evidence from computing devices in a manner suitable for presentation in a court of law.
Prerequisite:	Computer Information Systems 13 with a minimum grade of C or equivalent experience
Co-requisite:	
Recommended Preparation:	Computer Information Systems 119
Enrollment Limitation:	
Hours Lecture (per week):	2
Hours Laboratory (per week):	3
Outside Study Hours:	4
Total Course Hours:	90
Course Units:	3
Grading Method:	Letter Grade only
Credit Status:	Credit, degree applicable
Transfer CSU:	Yes
Effective Date:	12/17/2018
Transfer UC:	Yes
Effective Date:	
General Education: ECC	
Term:	
Other:	
CSU GE:	

Term:	
Other:	
IGETC:	
Term:	
Other:	
Student Learning Outcomes:	**SLO #1** Understand the role of the cybersecurity forensics investigator, and the concepts and terminology used in computer forensics. **SLO #2** Demonstrate the ability to use forensics tools to gather and analyze data on a compromised computer system. **SLO #3** Demonstrate the ability to conduct a forensics investigation. **SLO #4** Understand the complexities involved in conducting forensics investigations on various devices and in the cloud.
Course Objectives:	1. Compare and contrast the differences between cybercrimes against individuals, organizations, and society at large. 2. Identify the essential elements of a cybercrime, including the various modes and manners in which they are conducted. 3. Demonstrate how to obtain, analyze, interpret, and document computer forensic evidence for use in legal and computer security proceedings. 4. Demonstrate digital forensics investigation skills, and use digital forensic hardware and software tools to gather evidence to complete a digital forensic investigation. 5. Learn how to obtain, analyze, interpret, and document digital forensic evidence for use in legal and computer security proceedings. 6. Learn digital forensics investigation skills, and use digital forensic hardware and software tools to gather evidence to complete a digital forensic investigation.
Major Topics:	**I. Digital Forensics and Investigation (3 hours, lecture)** A. Understand Case Law B. Preparing for Computer Investigations C. Principles of Security **II. Forensics Investigation Processes (6 hours, lecture)** A. Systematic approach B. Goals of Investigation C. Conducting an investigation 1. File Systems A. Windows B. Linux and Mac 2. Windows Artifacts 3. Hidden Files

4. Hash Data

III. The Investigators Laboratory (3 hours, lecture)
A. Lab layout
B. Lab components
C. Organizational structure
D. Workstation tools
E. Toolkits for evidence collection

IV. Current Forensic Tools (3 hours, lecture)
A. Evidence acquisition
B. Analysis tools
C. Hex editor
D. Password crackers

V. Processing a Crime Scene (3 hours, lecture)
A. Prepare for a search
   1. Drive Letters in Linux
B. Seize digital evidence
   1. Image Process
C. Store digital evidence

VI. Data Acquisition (3 hours, lecture)
A. Tools to acquire digital evidence
   1. Autopsy Forensic Browser
B. Browser Artifacts Analysis
   1. Internet Explorer
   2. Mozilla Firefox
   3. Google Chrome

VII. Virtual Machine Forensics (3 hours, lecture)
A. Understand virtual machines
B. Live Acquisitions
C. Network Forensics

VIII. Recover Image Files (3 hours. lecture)
A. Data compression
B. Locate and Recover image files
   1. File Allocation Table (FAT) Partition
   2. New Technology File System (NTFS) Partition
   3. Memory Analysis

IX. Email Investigation (3 hours. lecture)
A. Investigate Email Crimes and Violations
   1. Network Traffic Emails
   2. View Email headers
   3. Trace Email
B. Specialized Email Forensic Tools
   1. Operating System (OS) Forensics
   2. Hex Editor

X. Mobile Forensics (3 hours, lecture)
A. Understanding Mobile device forensics

1. Mobile Phone Basics
    A. Subscriber Identity Module (SIM) card
    B. Short Message Service (SMS)
    C. Multimedia Messaging Service (MMS)
  2. Inside mobile devices
B. Understanding Acquisition Procedures for Mobile Devices
  1. Mobile Forensic Equipment

XI. Cloud Forensics (3 hours, lecture)
A. Understand Cloud Computing
  1. Cloud Service Levels
  2. Cloud Vendors
  3. Cloud tools
B. Legal Challenges
  1. Service Level Agreement
  2. Jurisdiction Issues

XII. Digital Forensics Fundamentals (6 hours, lab)
A. File Systems
  1. Window File System
  2. Linux File System
B. Windows Artifacts
  1. Event Logs
  2. Internet Information System Logs

XIII. Digital Forensics Fundamentals (6 hours, lab)
A. Hash Data Sets
  1. Encase Imager
  2. Hash Algorithm 1 (HA1)
B. Forensic Tools
  1. Foremost
  2. HEX

XIV. Evidence Acquisition, Preparation and Preservation (4 hours, lab)
A. Drive letters in Linux
  1. Primary Partitions
  2. Extended Partitions

XV. Evidence Acquisition, Preparation and Preservation (6 hours, lab)
A. Image Process
  1. FTK Imager
  2. HELIX
  3. Kali
B. Autopsy Artifacts
  1. Browser Artifacts

XVI. File and Program Activity Analysis (4 hours, lab)
A. FAT Partition
B. NTFS Partition
C. Memory Analysis

XVII. Browser Artifact Analysis (6 hours, lab)
A. Internet Explorer

	B. Google Chrome C. Mozilla Firefox **XVIII. Virtual Machine (4 hours, lab)** A. Type 1 Hypervisor B. Type 2 Hypervisor C. Live Acquisition **XIX. Communication Artifacts (6 hours, lab)** A. Email Messages B. Network Traffic Emails C. Network Forensic Analysis Tool (NFAT) Network Manager **XX. Mobile Forensics (6 hours, lab)** A. File structure B. SIM C. SMS D. MMS **XXI. Cloud Forensics (6 hours, lab)** A. Tools B. Recover files C. Recover Graphics
Total Lecture Hours:	36
Total Laboratory Hours:	54
Total Hours:	90
Primary Method of Evaluation:	2) Problem solving demonstrations (computational or non-computational)
Typical Assignment Using Primary Method of Evaluation:	You've recently been hired by the Signal Hill Police Department as their digital forensics intern. The first week you've been sent away for training in Las Vegas. During a noisy night out with your new buddies from the training center, you get a call from Lt. Zari. As you step into a bathroom stall to take the call, the Lt. explains the situation: A local drug dealer was arrested in his home. He had a five-year-old PC running Windows 7 and an iPhone in his possession at the time of the arrest. Because he was arrested with these electronics, search warrants are not an issue. In a one- to two-page report, document the following: What should your instructions be for the collection of data from the PC? Be very specific as these instructions are to be followed by non-professionals. Remember to give justifications for each step.
Critical Thinking Assignment 1:	Joshua Zarkan found his girlfriend's dead body in her apartment and reported it. The first responding law enforcement officer seized a USB drive. A crime scene evidence technician skilled in data acquisition made an image of the USB drive with ProDiscover and named it ClPrj01.eve. Following the acquisition, the technician transported and secured the USB drive and placed it in a secure evidence locker at the police station. You have received the

	image file from the detective assigned to this case. He directs you to examine it and identify any evidentiary artifacts that might relate to this case. In a one- to two-page report, explain how you are going to process the case. Once the case has been processed, export any files in the image and give them to the investigator. In addition, write a report including any facts from the contents of the recovered data.
Critical Thinking Assignment 2:	In this project, you work for a large corporation's IT security company. Your duties include conducting internal computing investigations and forensics examinations on company computing systems. A paralegal from the Law Department, Ms. Hidalgo, asks you to examine a USB drive belonging to an employee who left the company and now works for a competitor. The Law Department is concerned that the former employee might possess sensitive company data. Ms. Hidalgo wants to know whether the USB drive contains anything significant. In addition, she informs you the former employee might have had access to confidential documents because a co-worker saw him accessing his manager's computer on the last day of work. In a one- to two-page page report, respond to the following: Can you legally search the flash drive without a warrant? Are you breaking any laws or violating rights by searching someone's USB drive without consent? How can you legally search the USB drive for evidence? If you decide to search the USB drive, how will you process with this case?
Other Evaluation Methods:	Laboratory Reports, Multiple Choice, Other Exams, Quizzes
Instructional Methods:	Lab, Lecture, Multimedia presentations, Other (specify)
If other:	
Work Outside of Class:	Problem solving activity, Required reading, Study, Written work (such as essay/composition/report/analysis/research)
If Other:	
Up-To-Date Representative Textbooks:	Nelson, Phillips, Steuart, Guide to Computer Forensics and Investigations, 6th ed., Course Technology, 2019.
Alternative Textbooks:	Marjie Britz, Computer Forensics and Cyber Crime: An Introduction, 3rd ed., Prentice Hall, 2013. (Discipline Standard)
Required Supplementary Readings:	
Other Required Materials:	USB 2.0 flash drive 8 GB or larger
Requisite:	Prerequisite
Category:	sequential
Requisite course(s): List both prerequisites	Computer Information Systems 13 with a minimum grade of C or

and corequisites in this box.	
Requisite and Matching skill(s):Bold the requisite skill. List the corresponding course objective under each skill(s).	**Demonstrate an understanding of the development and use of information systems in business.** CIS 13 - Explain the development and use of information systems in business. **Identify the impact of the expanding scope of digital technology including career opportunities, privacy, security, ethics, global relationships, and perceptions of reality.** CIS 13 - Identify and analyze existing and emerging technologies and their impact on organizations and society including computer, communication and information systems, privacy, security, crime, ethics, global relationships, and career opportunities.
Requisite Skill:	equivalent experience
Requisite Skill and Matching Skill(s): Bold the requisite skill(s). If applicable	A student having equivalent experience would have a knowledge of computer hardware, software, and computer security systems, and be able to research the problems and reach conclusions using a variety of resources, including the Internet.
Requisite course:	Computer Information Systems 119
Requisite and Matching skill(s):Bold the requisite skill. List the corresponding course objective under each skill(s).	**Demonstrate the ability to analyze and document a network configuration, and identify security risks.** CIS 119 - Understand the challenges of securing information. CIS 119 - Apply knowledge of computer hardware, software, file systems and networks in identifying and resolving computer crime and information security incidents.
Requisite Skill:	
Requisite Skill and Matching skill(s): Bold the requisite skill. List the corresponding course objective under each skill(s). If applicable	
Enrollment Limitations and Category:	
Enrollment Limitations Impact:	
Course Created by:	Richard Perkins
Date:	04/25/2018
Original Board Approval Date:	
Last Reviewed and/or Revised by:	
Date:	
Last Board Approval Date:	12/19/2022