Cosumnes River College
CISS 360
Computer Forensics and Investigation
A Hybrid-Online Course
Fall 2017
(2nd 8 weeks)

Instructor: Buddy Spisak **Office Hours**: Mon. 6:00-7:00 p.m. (Aug. 21 to Dec. 11)

Office: BSS-143
Voice Mail: (916) 286-3691 ext. 14162
Email: spisakj@crc.losrios.edu The turnaround time for responding to most emails is about one to two days. Be sure to include your name and the course number in each email so I can identify who you are and what the email is about.
Course Web page: https://canvas.losrios.edu/
Instructor Web page: http://crc.losrios.edu/spisakj/

Prerequisites: CISS 310
Advisory: CISS 308
Lecture: Online
Laboratory: Th 6:00 to 9:05pm in BS-153
Accepted for Credit: CSU
Class Credits: 3 units

Required Textbook:

Title:	*Guide to Computer Forensics and Investigations*, 5th ed.
Authors:	Bill Nelson, Amelia Phillips, and Christopher Steuart
Publishing Info:	Cengage Learning, 2016
Textbook ISBN13:	978-1-285-06003-3
E-Book ISBN13:	978-1-305-80568-2

Optional Materials: A flash drive to store your work for the class

Course Description:

This course is an introduction to the methods used to properly conduct a computer forensics investigation and begins 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.

Student Learning Outcomes and Course Objectives:

- REVIEW OF THE COMPUTER FORENSICS PROFESSION (SLO #01)
  - Illustrate how to prepare for computer investigations and explain the difference between law enforcement agency and corporate investigations.
  - Explain how other organizations' codes of ethics apply to expert testimony.
- SUMMARIZE HOW TO PREPARE FOR A COMPUTER INVESTIGATION (SLO #02).
  - Apply a systematic approach to an investigation.

    - Describe procedures for corporate high-tech investigations.
    - Explain requirements for data recovery workstations and software.
    - Describe how to conduct an investigation.
- SUMMARIZE THE CERTIFICATION REQUIREMENTS FOR COMPUTER FORENSICS LABS (SLO #03).
    - Catalog the physical requirements for a computer forensics lab.
    - Draft the criteria for selecting a basic forensic workstation.
- MEASURE THE DIFFERENT WAYS FOR PROPER DATA ACQUISITION (SLO #04).
    - Summarize the different digital evidence storage formats being used today.
    - Explain ways to determine the best acquisition method.
    - Explain how to use acquisition tools properly.
    - Explain how to validate data acquisitions.
- CLASSIFY THE RULES FOR PROPER DIGITAL EVIDENCE HANDLING (SLO #05).
    - Describe how to collect evidence at private-sector incident scenes.
    - Explain guidelines for processing law enforcement crime scenes.
    - Review a case to identify requirements and plan your investigation.
- ANALYZE HOW DATA IS STORED AND MANAGED ON AN OPERATING SYSTEMS (SLO #06).
    - Analyze an operating system's file structure.
- ANALYZE SOME OF THE DIFFERENT COMPUTER FORENSICS TOOLS (SLO #07).
    - Explain how to evaluate needs for computer forensics tools.
    - Describe methods for validating and testing computer forensics tools.
- VALIDATE THE EVIDENCE DURING THE ANALYSIS PROCESS (SLO #08).
    - Describe methods of performing a remote acquisition.
    - Determine what data to analyze in a computer forensics investigation.
    - Integrate the necessary tools to validate data and for the most common data-hiding techniques.
- IDENTIFY AND RECONSTRUCT GRAPHICS FILES (SLO #09).
    - Summarize the different types of graphics file formats being used today and describe how to identify unknown ones.
    - Explain types of data compression and how to locate and recover graphics files.
    - Summarize the copyright issues associated with graphic files.
- DESCRIBE THE IMPORTANCE OF NETWORK FORENSICS (SLO #10).
    - Illustrate the primary concerns in conducting forensic examinations of virtual machines.
    - Analyze the standard procedures for performing a live or network acquisition.
- ANALYZE EMAIL INVESTIGATIONS (SLO #11).
- GENERATE A FORENSIC REPORT (SLO #12).
    - Explain the importance of reports.
    - Describe guidelines for writing reports.
    - Explain how to use forensics tools to generate reports.
- DESCRIBE GUIDELINES FOR TESTIFYING IN COURT (SLO #13).
    - Summarize the guidelines for testifying in depositions and hearings.

Methods of Measuring Student Learning Outcomes:

- You will demonstrate knowledge of network and internet security applications and standards through class discussions and achievement on quizzes and final examination.
- You will demonstrate competence in the coursework by completing projects and participating in discussions during the semester.

Student Obligations:

- **Attendance**: Since this course is online, only attendance at the On-Campus Orientation on October 19 and the Final on December 7 is necessary. There will be weekly lab time on campus, and it is up to you to complete the lab assignments during the lab time or at home.
- **Discussions**: I want everyone to take a pro-active approach to learning this material. This includes using the Discussions link to ask questions and also answer other students' questions. I will also post questions each week that you can answer to further your understanding of the material. I expect two postings each week unless otherwise noted.
- **Projects**: There will be six hands-on projects and six case projects credited for homework for the class. The projects will help reinforce what you are learning in each lesson. The due dates are located in the **SCHEDULE** portion of this handout. You will submit your results into the Canvas discussions area in order to receive points for that assignment. On all projects you are expected to do your own work.
- **Quizzes**: After each lesson you will be required to take a short quiz, which will test you on the material covered. It is open-book and open-notes. You can take the quiz multiple times to improve your score, but be aware that the questions will change each time and that your most recent score will be the one counted as the grade.
- **Final Exam**: The final exam will consist of two parts. One part of the exam will be a hands-on practical demonstration of assigned tasks, and the other part will be an exam taken in Canvas.
- **Late Work**: Unless noted, all assignments are due on Sunday by midnight each week. Late work will be accepted ONLY if you have contacted me prior to the due date either by email or voice mail. In general, late work is due the next week, and no late assignments may be turned in after one week from the original due date, regardless of the reason. For every day an assignment is late, you will lose 10% of its grade.
- **Due Dates**: Unless noted, all assignments will be submitted in Canvas. If, for any reason, you cannot access Canvas or are unable to submit the assignment on time, please email it to me instead so that you are not penalized for being late. Quizzes cannot be taken, nor can discussion items be completed after their due dates. If you miss a quiz and you want to make up points, you can take advantage of the extra credit assignments posted in Canvas. Everyone is welcome to work on the extra credit assignments. Typically, they are five to ten points each, depending on the difficulty of the assignment.
- **Plagiarism Policy**: It is inappropriate, and a violation of academic policy, to copy information from any source (including, but not limited to, textbooks, magazine articles, newspaper articles and internet articles) without giving proper credit to the author by using standard quotation procedures such as in-line quotes, footnotes, endnotes, etc. Quotes may not exceed 25% of the assignment's total length. You will receive no credit (0 points) for any assignment that copies any material from any other source without giving proper credit to the author(s). Repeat offenders of this policy are subject to academic discipline as outlined in the policies published by the college.
- **Cheating**: Students who cheat will receive a failing grade for the course. [See the Student Behavior and Academic Integrity page of the college website (https://www.crc.losrios.edu/catalog/geninfo/integrity).]
- **CRC Honor Code:** Academic integrity requires honesty, fairness, respect and responsibility. [See the Cosumnes River College Honor Code posted on the college website (https://www.crc.losrios.edu/facstaff/resourceguide/faculty/student-behavior-academic-integrity/honorcode - https://www.crc.losrios.edu/facstaff/resourceguide/faculty/student-behavior-academic-integrity/honorcode)].
- **Email**: Every student will be required to have an email account. If you do not have an email account, the college provides free email accounts for all current students. To activate your account, go to https://apps.losrios.edu/login.html and follow the directions provided.
- **Email etiquette**: I will not tolerate rude and demeaning comments or emails to anyone in this class. Please keep your comments and emails topic-related. If I determine that a comment or email to anyone else in the class is rude or demeaning, I will warn you once. If your behavior

continues to be unacceptable, I will refer you to the administration of the college for disciplinary action.

- **Personal belongings**: No food or drinks are allowed in the classroom. All cell phones, beepers, pagers, etc. should be turned off or set to vibrate.
- **Disabilities:** If you have a documented disability and wish to discuss academic accommodations, please contact me or contact the Office of Disabled Student Programs and Services at 691-7275 as soon as possible.
- **Campus Police**: You can call 558-2221 to request a safety escort.
- **Canvas:** This class utilizes a product called "Canvas." It is highly recommended that you check the website frequently for scheduling updates and homework assignments. Most of the homework assignments and quizzes will be done on Canvas.
- **Course Responsibilities:** This course requires significant self-motivation. You must not get behind. Labs and weekly assignments can take up to eight hours to finish. Please don't try to finish them in one day. Not all activities are created equal. Some may take a bit longer than others. You would normally spend 3 hours per week in class for this course: total of 54 hours. Allow yourself at least 8 hours per week to complete the activities online, including the time spent writing for the postings to the discussions page. You should plan additional time to read the textbook and study for the quizzes. Some people believe this is a much easier way to study this subject than an on-campus framework because they love to read and avoid the parking problems. Others feel very intimidated at first. Be patient as you work your way through the activities.

Grading:

Course Topic		Points	Total	Approximate % the of Grade
Hands-on Projects (7)		50	350	30
Case Projects (7)		20	140	13
Orientation Quiz (1)		10	10	1
Quizzes (7)		30	210	19
Discussions (7)		20	140	13
Final Exam (1)		200	200	24

Point System: There are 1050 total assigned points.

Grade Ranges: A= 945-1050, B=840-944, C=735-839, D=630-734, F=0-629

Schedule: It is tentative and can change during the course for the term (continues on p. 6).

Week:	Day:	Date:	Proposed Schedule:	Assignment Due:	Due Date (By Midnight):
Week 1	Thurs.	10/12	Orientation and Introductions		Sun., Oct. 22
			View the Online Orientation	Orientation Quiz	
			Read Ch 1: Understanding the Digital Forensics Profession and Investigations Read Ch 2: The Investigator's Office and Laboratory	Discussion #1	
			Do all Hands-on Projects and one Case Project from either Chapter 1 or 2	Quiz #1	
				Hands-on Project #1	
				Case Project #1	
Week 2	Thurs.	10/19	Read Ch 3: Data Acquisition Read Ch 4: Processing Crime and Incident Scenes	Discussion #2	Sun., Oct. 29
			Do all Hands-on Projects and one Case Project from Chapter 3 or 4	Quiz #2	
				Hands-on Project #2	
				Case Project #2	
Week 3	Thurs.	10/26	Read Ch 5: Working with Windows and CLI Systems Read Ch 6: Current Computer Forensics Tools	Discussion #3	Sun., Nov. 5
			Do all Hands-on Projects and one Case Project from Chapter 5 or 6	Quiz #3	
				Hands-on Project #3	
				Case Project #3	
Week 4	Thurs.	11/2	Read Ch 7: Macintosh and Linux Boot Processes and File Systems Read Ch 8: Recovering Graphics Files	Discussion #4	Sun., Nov. 12
			Do all Hands-on Projects and one Case Project from Chapter 7 or 8	Quiz #4	
				Hands-on Project #4	
				Case Project #4	
Week 5	Thurs.	11/9	Read Ch 9: Computer Forensics Analysis and Validation Read Ch 10: Virtual Machine and Cloud Forensics	Discussion #5	Sun., Nov. 19
			Do all Hands-on Projects and one Case Project from Chapter 9 or 10	Quiz #5	
				Hands-on Project #5	
				Case Project #5	
Week 6	Thurs.	11/16	Read Ch 11: Live Acquisitions and Network Forensics Read Ch 12: Email investigations	Discussion #6	Sun. Nov. 26
			Do all Hands-on Projects and one Case Project from Chapter 11 or 12	Quiz #6	
				Hands-on Project #6	
				Case Project #6	
	Thurs.	11/23	Thanksgiving Break (campus closed Nov. 23-24)		
Week 7	Thurs.	11/30	Read Ch 14: Report Writing for High Tech Investigations Read Ch 15: Expert Testimony in High Tech Investigations	Discussion #7	Sun. Dec. 3
			Do all Hands-on Projects and one Case Project	Quiz #7	

			from Chapter 14 or 15		
				Hands-on Project #7	
				Case Project #7	
Week 8	Thurs.	12/7	Final Exam		Sun. Dec. 10