COWLEY COLLEGE
& Area Vocational Technical School

COURSE PROCEDURE FOR

INTRODUCTION TO COMPUTER FORENSICS
CIS1881 3 Credit Hours

Student Level:
This course is open to students on the college level in either the freshman or sophomore year.

Catalog Description:

CIS1881 – INTRODUCTION TO COMPUTER FORENSICS (3 hrs)
A course to give students an introduction to computer forensics including hardware and software components along with evidence gathering. Students will use various computer forensics software to analyze data. Prerequisite: Basic computer skills.

Prerequisites: Basic computer skills.

Controlling Purpose:
This course is designed to introduce students to computer forensics. Students will learn how to use various computer forensics software to analyze digital evidence and search for hidden data. Various computer fundamentals will be covered.

Learner Outcomes:
Upon completion of the course, the student will be able to use various computer forensics software to analyze information on a computer system. The student will understand how information is stored on the hard drive and in system files.

Units Outcomes and Criterion Based Evaluation Key for Core Content:
The following defines the minimum core content not including the final examination period. Instructors may add other content as time allows.

Evaluation Key:

A = All major and minor goals have been achieved and the achievement level is considerably above the minimum required for doing more advanced work in the same field.

B = All major goals have been achieved, but the student has failed to achieve some of the less important goals. However, the student has progressed to the point where the goals of work at the next level can be easily achieved.

C = All major goals have been achieved, but many of the minor goals have not been achieved. In this grade range, the minimum level of proficiency represents a person who has achieved the major goals to the minimum amount of preparation necessary for taking more advanced work in the same field, but without any major handicap of inadequacy in his background.

D = A few of the major goals have been achieved, but the student's achievement is so limited that he is not well prepared to work at a more advanced level in the same field.
F = Failing, will be computed in GPA and hours attempted.
N = No instruction or training in this area.

UNIT 1: COMPUTER FORENSICS AND INVEWTIGATIONS AS A PROFESSION Outcomes: Understand what is computer forensics and investigations and some problems/concerns prevalent in the industry						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain what is computer forensics
						Explain the preparation process for computer investigations
						Explain professional conduct in regards to computer forensics

UNIT 2: UNDERSTANING COMPUTER INVESTIGATIONS Outcomes: Understand how to manage a computing investigation						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain the concepts involved in preparing a computer investigation
						Explain the systematic approach
						List the procedures for corporate high-tech investigations
						Explain data recovery workstations and software
						List and explain the steps in conducting an investigation
						Explain completing the case

UNIT 3: THE INVESTIGATOR'S OFFICE AND LABORATORY Outcomes: Understand how to set up an effective computer forensics laboratory						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain forensics lab certification requirements
						Explain determining the physical requirements for a computer forensics lab
						Explain selecting a basic forensic workstation
						Explain building a business case for developing a forensics lab

UNIT 4: DATA AQUISITION Outcomes: Understand how to perform static acquisitions from digital media						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						List and explain the storage formats for digital evidence
						Explain how to determine the best acquisition method
						Explain contingency planning for image acquisition
						Use acquisition tools
						Validate data acquisitions
						Explain RAID data acquisitions
						Use remote network acquisition tools
						Use misc forensics acquisition tools

UNIT 5: PROCESSING CRIME AND INCIDENT SCENES Outcomes: Understand how to process a computer investigation scene						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain the identification of digital evidence
						Explain collecting evidence in private-sector incident scenes
						Explain how to prepare for a search
						Explain how to secure a computer incident or crime scene
						Explain how to seize digital evidence at the scene
						Explain how to store digital evidence
						Explain how to obtain a digital hash and what it means
						Explain how to review a case

UNIT 6: WORKING WITH WINDOWS AND DOS SYSTEMS Outcomes: understand how data is stored and managed on Microsoft operating systems						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain file Systems Concepts
						Explain how to examine NTFS disks
						Explain the purpose of the windows registry
						Explain the purpose of Microsoft Startup tasks
						Explain the purpose of MS-DOS startup tasks
						Explain the purpose of virtual machines

UNIT 7: CURRENT COMPUTER FORENSICS TOOLS Outcomes: Understand how to use various software and hardware tools used during computer forensics investigations						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Evaluate computer forensics tool needs
						Use computer forensics software tools
						Use computer forensics hardware tools
						Explain how to validate and test forensics software

UNIT 8: MACINTOSH AND LINUX BOOT PROCESSES AND FILE SYSTEMS Outcomes: Understand the basics of Macintosh and Linux boot processes and file systems						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain the Macintosh file structure and boot process
						Examine UNIX and Linux disk structures and boot processes
						Explain other disk structures such ad CD, SCSI, IDE/EIDE and SATA

UNIT 9: COMPUTER FORENSICS ANALYSIS AND VALIDATION Outcomes: Understand how to apply computer forensics topics and techniques to a computing investigation						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain what data to collect and analyze
						Explain how to validate forensic data
						Explain data-hiding techniques and use tools associated with data-hiding
						Explain how to perform remote acquisition

UNIT 10: RECOVERING GRAPHIC FILES Outcomes: Understand the techniques for recovering graphic files						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Recognize a graphics file
						Explain data compression
						Locate and recover graphics files
						Identify unknown file formats
						Explain copyright issues with graphics

UNIT 11: VIRTUAL MACHINES, NETWORK FORENSCIS, AND LIVE ACQUISITIONS Outcomes: Understand the uses of virtual machines network forensics and how to perform a live acquisition						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain the concept of virtual machines
						Explain the concept of network forensics
						Perform a live acquisition
						Explain standard procedures for network forensics
						Use network tools including UNIX/Linux tools, packet sniffers
						Explain the Honeynet project

UNIT 12: E-MAIL INVESTIGATIONS Outcomes: Understand how to trace, recover and analyze e-mail messages by using forensics tools						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain the role of E-mail in investigations
						Explain the roles of the client and server in e-mail
						Investigate e-mail crimes and violations (simulated)
						Explain e-mail server basic concepts
						Use specialized e-mail forensics tools

UNIT 13: CELL PHONE AND MOBILE DEVICE FORENSICS Outcomes: Understand how to retrieve information from a cell phone or mobile device						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain the basics of mobile device forensics
						Explain acquisition procedures for cell phones and mobile devices

UNIT 14: REPORT WRITING FOR HIGH –TECH INVESTIGATIONS Outcomes: Understand the guidelines on writing reports of your findings in computer forensics investigations						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain the importance of reports
						List and explain the guidelines for writing reports
						Generate report findings with forensics software tools

UNIT 15: EXPERT TESTIMONY IN HIGH –TECH INVESTIGATIONS Outcomes: Understand the rules of evidence and procedure as they apply to testimony						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain the preparation steps for testimony
						Explain testifying in court
						Explain the preparation for a deposition or hearing
						Explain the preparation of forensic evidence for testimony

UNIT 16: ETHICS FOR THE EXPERT WITNESS Outcomes: Understand applying ethics and codes of conduct to computer forensics and testimony						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain the role of ethics and codes in regards to expert witnesses
						List the organizations with code of ethics
						Explain ethical difficulties in expert testimony

Projects Required:
None.

Textbook:
Contact Bookstore for current textbook.

Materials/Equipment Required:

Attendance Policy:
Students should adhere to the attendance policy outlined by the instructor in the course syllabus.

Grading Policy:
The grading policy will be outlined by the instructor in the course syllabus.

Maximum class size:
Based on classroom occupancy

Course Timeframe:
The U.S. Department of Education, Higher Learning Commission and the Kansas Board of Regents define credit hour and have specific regulations that the college must follow when developing, teaching and assessing the educational aspects of the college. A credit hour is an amount of work represented in intended learning outcomes and verified by evidence of student achievement that is an institutionally-established equivalency that reasonably approximates not less than one hour of classroom or direct faculty instruction and a minimum of two hours of out-of-class student work for approximately fifteen weeks for one semester hour of credit or an equivalent amount of work over a different amount of time. The number of semester hours of credit allowed for each distance education or blended hybrid courses shall be assigned by the college based on the amount of time needed to achieve the same course outcomes in a purely face-to-face format.

Refer to the following policies:

402.00 Academic Code of Conduct
263.00 Student Appeal of Course Grades
403.00 Student Code of Conduct

Disability Services Program:

Cowley College, in recognition of state and federal laws, will accommodate a student with a documented disability. If a student has a disability, which may impact work in this class which requires accommodations, contact the Disability Services Coordinator.