ILLINOIS VALLEY COMMUNITY COLLEGE

COURSE OUTLINE

DIVISION: Workforce Development

COURSE: CSC 2200 Digital Forensics

Date: Fall 2021

Credit Hours: 3

Prerequisite(s): CSO 2200, CSO 2202, CSN 1225

Delivery Method:		
☒ **Lecture**	**2 Contact Hours (1 contact = 1 credit hour)**
☐ **Seminar**	**0 Contact Hours (1 contact = 1 credit hour)**
☒ **Lab**	**2 Contact Hours (2-3 contact = 1 credit hour)**
☐ **Clinical**	**0 Contact Hours (3 contact = 1 credit hour)**
☒ **Online**	
☐ **Blended**	
☒ **VCM**	

Offered: ☐ **Fall** ☒ **Spring** ☐ **Summer**

CATALOG DESCRIPTION and IAI NUMBER (if applicable):
This course instructs the student in how to discover, identify, extract and document computer crimes and corporate policy violations. The student performs this work by analyzing computer data through digital forensic tools.

ACCREDITATION STATEMENTS AND COURSE NOTES:
None

COURSE TOPICS AND CONTENT REQUIREMENTS:
1. Computer Forensics Scope and Definition
2. Data Acquisition and Handling
3. Online Investigations
4. Documenting the Evidence
5. Network Forensics
6. Mobile Forensics
7. Recovering Graphic Files
8. Report Writing

INSTRUCTIONAL METHODS:
1. Lecture
2. Discussion
3. Readings
4. Case Studies
5. Hands-On Forensic Labs

EVALUATION OF STUDENT ACHIEVEMENT:
Students must:
1. Participate in class discussions or demonstrate by work completed the recorded videos of class were reviewed
2. Complete readings, assignments, quizzes, exams, hands-on forensic labs, and other assignments given at the instructor's discretion
3. Ask questions about any misunderstood area either in class, during office hours, or of the tutor.

A = 90 – 100
B = 80 – 89
C = 70 – 79
D = 60 – 69
F = 0 – 59

INSTRUCTIONAL MATERIALS:
Textbooks
Textbooks used in Digital Forensics are at the discretion of full-time faculty.

Part-time faculty members are to use the textbook designated for Digital Forensics by the Program Coordinator for Cybersecurity and the Dean of Workforce Development.

Resources
FTK Case Study & Software
Autopsy Case Study

Computer Applications:
1. Word Processing software
2. Access Data FTK ToolKit
3. Online Course Management Software
4. IVCC email account

Other:
1. Audio/video resources
2. USB with additional software installed
    a. TeamViewer
    b. Autopsy
    c. Case Study

LEARNING OUTCOMES AND GOALS:
Institutional Learning Outcomes

☐ ILO 1: Communication – to communicate effectively;
☒ ILO 2: Inquiry – to apply critical, logical, creative, aesthetic, or quantitative analytical reasoning to formulate a judgement or conclusion;
☐ ILO 3: Social Consciousness – to understand what it means to be a socially conscious person, locally and globally;
☐ ILO 4: Responsibility – to recognize how personal choices affect self and society.

Course Outcomes and Competencies

Outcome 1: Identify the scope of computer forensics.
Competency 1.1: The student will be able to identify the types of forensics evidence recovered including email, images, video, internet searches, website visits, cell phone
Competency 1.2: The student will be able to understand the importance of computer forensics across industries

Outcome 2: Know the fundamental technology behind operating systems and file systems
Competency 2.1: The student will be able to define an operating system
Competency 2.2: The student will be able to convert between binary, decimal, and hexadecimal notation
Competency 2.3: The student will be able to identify the physical structure of a hard drive and how files are stored and retrieved
Competency 2.4: The student will be able to understand the booting process

Outcome 3: Understand the use of computer hardware storage media in computer forensic investigations
Competency 3.1: The student will be able to understand the types of devices used to forensically extract data from different storage devices.
Competency 3.2: The student will be able to understand how evidence should be handled and analyzed
Competency 3.3: The student will be able to understand the use of storage media in actual investigations.

Outcome 4: Determine how to set up a secure forensics lab
Competency 4.1: The student will be able to identify good practices for managing and processing evidence in a computer forensics lab
Competency 4.2: The student will be able to know how to properly acquire, handle, and analyze digital evidence
Competency 4.3: The student will be able to use UNIX commands to scour files for particular information of interest.

Outcome 5: Understand how to thoroughly document the forensic investigation
Competency 5.1: The student will be able to obtain/seize evidence and handle it properly
Competency 5.2: The student will be able to document the investigation though forensic tools and reports
Competency 5.3: The student will be able to understand what digital evidence and reporting is required for legal systems

Outcome 6: Identify and document network breaches
Competency 6.1: The student will be able to understand the importance of network forensics and the underlying structure of networks
Competency 6.2: The student will be able to investigate a network intrusion

Outcome 7: Identify and document mobile forensics.
Competency 7.1: The student will be able to understand the types of evidence available from cellphone carriers
Competency 7.2: The student will be able to retrieve evidence from a smart phone
Competency 7.3: The student will be able to analyze cell phone operating systems.

Outcome 8: Understand photograph forensics.
Competency 8.1: The student will be able to understand different types of digital photograph files and the metadata associated with these files.
Competency 8.2: The student will be able to analyze photographic images by social media users.