ILLINOIS VALLEY COMMUNITY COLLEGE

COURSE OUTLINE

DIVISION: Workforce Development

COURSE: CSC 2200 Digital Forensics

Date: Fall 2022

Credit Hours: 3

Complete all that apply or mark "None" where appropriate:
        Prerequisite(s): CSO 2200, CSN 1225

        Enrollment by assessment or other measure? ☐ Yes ☐ No
        If yes, please describe:

        Corequisite(s): None

        Pre- or Corequiste(s): None

        Consent of Instructor: ☐ Yes ☒ No

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**
                                  ☒ **Virtual Class Meeting (VCM)**

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

CATALOG DESCRIPTION and IAI NUMBER (if applicable):
This class is designed to provide students with the skills and standards for entry-level information security specialists in computer forensics measures. The student performs this work by analyzing computer data through digital forensic tools. At the end of this class, the student will be prepared to sit for EC-Council Digital Forensics Essentials Certification Exam.

ACCREDITATION STATEMENTS AND COURSE NOTES:
None

COURSE TOPICS AND CONTENT REQUIREMENTS:
1. Computer Forensics Fundamentals
2. Computer Forensics Investigation Process
3. Understanding Hard Disks and File Systems
4. Data Acquisition and Duplication
5. Defeating Anti-forensics Techniques
6. Windows Forensics
7. Linux and MAC Forensics
8. Network Forensics
9. Investigating Web Attacks
10. Dark Web Forensics
11. Investigating Email Crimes
12. Malware Forensics

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 Imaging

Autopsy Tools
Autopsy Case Study
EC-Council

Computer Applications:
1. Word Processing software
2. PowerPoint Software
3. Online Course Management Software
4. IVCC email account

Other:
1. Microphone on computer for online classes

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

Course Outcomes and Competencies
Outcome 1: Understand the basics of Computer Forensics Fundamentals.
Competency 1.1: The student will be able to discuss the fundamental concepts of
computer forensics, digital evidence, and forensic readiness.
Competency 1.2: The student will be able to understand the legal compliance issues
in computer forensics

Outcome 2: Understand the Computer Forensics Investigation Process
Competency 2.1: The student will be able to identify the computer investigation
process and phases
Competency 2.2: The student will be able to compute hashes of files and text strings
in the forensic process and determine if they are malicious

Outcome 3: Understand the use of computer hardware storage media & file systems in
computer forensic investigations
Competency 3.1: The student will be able to discuss the booting process of
Windows, Linux, and MAC operating systems
Competency 3.2: The student will be able to describe the logical structure of a disk
Competency 3.3: The student will be able to explain various file systems of
Windows, Linux, and MAC operating systems
Competency 3.4: The student will be able to successfully recover files that have
been permanently deleted

Outcome 4: Understand Data Acquisition Concepts
Competency 4.1: The student will be able to discuss different types of data
acquisition and formats

Outcome 5: Understand and examine various anti-forensics techniques and identify countermeasures
    Competency 5.1: The student will be able to discuss various types of anti-forensic techniques
    Competency 5.2: The student will be able to explain file carving on Windows and Linux systems
    Competency 5:3: The student will be able to crack passwords of password-protected files and applications

Outcome 6: Examine various volatile and non-volatile information-gathering techniques
    Competency 6.1: The student will be able to discuss the process of collecting volatile information and non-volatile information from a Windows system.
    Competency 6.2: The student will be able to explain how to perform Windows memory and registry analysis.
    Competency 6.3: Understand the difference between collecting data from a Linux system vs Windows
    Competency 6.4: Explain MAC forensics

Outcome 7: Understand network forensics
    Competency 7.1: The student will be able to discuss how to identify and analyze indicators of Compromise from network logs
    Competency 7.2: The student will be able to explain how to investigate network traffic for TCP SYN flooding, SYN-FIN flooding, and MAC flooding attempts
    Competency 7.3: The student will be able to explain various types of network-based evidence and various types of event correlation.

Outcome 8: Investigate Web Attacks
    Competency 8.1: The student will be able to understand web server logs
    Competency 8.2: The student will be able to perform web application forensics to detect and investigate various attacks on web applications

Outcome 9: Understand Dark Web Forensics
    Competency 9.1: The student will be able to discuss the working of the dark web

Outcome 10: Understand the process of investigating email crimes
    Competency 10.1: The student will be able to discuss the steps involved in investigating email crimes

Outcome 11: Understand malware forensics
    Competency 11.1: The student will be able to discuss malware forensic fundamentals
    Competency 11.2: The student will be able to explain how to analyze suspicious word documents
    Competency 11.3:   The student will be able to perform system behavior analysis.