CYBR C150: INTRODUCTION TO DIGITAL FORENSICS

Item	Value
Curriculum Committee Approval Date	10/27/2023
Top Code	070800 - Computer Infrastructure and Support
Units	3 Total Units
Hours	72 Total Hours (Lecture Hours 54; Lab Hours 18)
Total Outside of Class Hours	0
Course Credit Status	Credit: Degree Applicable (D)
Material Fee	No
Basic Skills	Not Basic Skills (N)
Repeatable	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

Students will explore an introduction to digital forensics using open source applications. Topics covered include chain of custody, forensic acquisition of data, forensic evidence reporting, expert witness testimony, timeline analysis, and anti-forensic techniques. Hands-on assignments will be used to develop introductory technical skills relevant to entry-level cybersecurity professionals. This course is intended for students with computer experience and an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated. ADVISORY: IT C104. Transfer Credit: CSU. C-ID: ITIS 165.**C-ID:** ITIS 165.

Course Level Student Learning Outcome(s)

1. Identify and collect digital evidence in an organized manner for reporting.
2. Demonstrate an understanding of chain of custody with regard to digital forensics.
3. Recognize the various professional specializations of cybersecurity, incident response, and digital forensics.

Course Objectives

- 1. Describe the digital forensics profession and trends in the field.
- 2. Describe emerging cybersecurity trends and the impact on digital forensics as a specialized field of study.
- 3. Explain how to use forensic tools to evaluate and examine digital evidence.
- 4. Demonstrate the use of digital forensics tools to perform an analysis of evidence in a mock case.
- 5. Share contemporary cases where digital forensic techniques are used to examine evidence and influence case outcomes.
- 6. Outline the history of digital forensics and provide historical case studies to define the evolution of the use of digital evidence in court.

Lecture Content

Computer Forensics as a Profession Understanding Computer Forensics Preparing for computer investigations Forensic specializations Digital Forensics Process and Procedures Use a systematic approach Chain of Custody regarding digital evidence Forensic data acquisitions Digital Forensics Analysis Evidence Collection - Windows artifacts Windows Registry Introduction to anti-forensics Introduction to timeline analysis Forensics Tools Windows based tools Open source and other tools Introduction to Linux tools Forensics Report Expert Witness Testimony

Lab Content

Students will work with remote lab environments to complete hands-on activities. Identify and collect digital evidence in an organized manner for reporting Follow chain of custody procedures used in the digital forensics profession Acquire data to create a forensically sound image Review Windows artifacts in the Windows registry Create a comprehensive report of evidence from the Windows registry Complete a timeline analysis Analyze evidence using open source forensics tools Create a comprehensive report of evidence from a forensic image

Method(s) of Instruction

- Lecture (02)
- DE Live Online Lecture (02S)
- DE Online Lecture (02X)
- Lab (04)
- DE Live Online Lab (04S)
- DE Online Lab (04X)

Instructional Techniques

This course will utilize a combination of lecture, hands-on guided laboratory assignments, classroom/discussion student interactions, problem solving, quizzes, tests, and troubleshooting assignments to achieve the goals and objectives of this course. All instructional methods are consistent across all modalities.

Reading Assignments

Read about and research the role of the computer forensics profession. Read about the digital forensics process and procedures. Conduct digital forensics analysis using Windows based tools resulting in a written report and expert witness testimony.

Writing Assignments

Complete an expert witness report of digital forensics analysis performed.

Out-of-class Assignments

Complete hands-on lab to conduct digital forensics analysis using Windows based tools. Complete hands-on lab to demonstrate proper digital forensics processes and procedures.

Demonstration of Critical Thinking

Students will conduct digital forensics analysis using best practices processes, and procedures.

Required Writing, Problem Solving, Skills Demonstration

Skills will be demonstrated through completion of hands-on lab exercises using Windows based forensics tools and document analysis performed in preparation for expert witness testimony.

Eligible Disciplines

Computer information systems (computer network installation, microcomputer ...: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience. Computer service technology: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience.

Textbooks Resources

1. Required Nelson, B.; Phillips, A.; and Steuart, C. Guide to Computer Forensics and Investigations, 7th ed. Boston: Cengage, 2024

Other Resources

1. Coastline Library 2. OER - Open Educational Resources