CYBR C250: INTERMEDIATE 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
Open Entry/Open Exit	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

Students will explore digital forensic techniques using industry-recognized tools. Topics covered include an introduction to network forensics and mobile device forensics, investigative and extraction tools, live acquisition data, evidence reporting, time-stomping and anti-forensic techniques, and the significance of time zones for forensic case analysis. Hands-on assignments will be used to develop 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 C04 and CYBR C150. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Evaluate a collection of digital evidence to distinguish and extract relevant items.
2. Given a simulated case, use a forensic framework or methodology to analyze and reconstruct the electronic events of the case.
3. Given a simulated case, analyze the evidence and produce a report to describe evidence and present findings.

Course Objectives

- 1. Describe the digital forensics investigation lifecycle.
- 2. Demonstrate the use of industry-recognized tools to perform a forensic analysis of a simulated case.
- 3. Demonstrate the techniques used to find time-stomping and anti-forensic techniques.

Lecture Content

Introduction to Digital Forensics Frameworks Checklist for entry-level analysts Investigative/extraction tools Linux-based tools SIFT workstation Types of forensic reviews Live data acquisition Mobile device forensics Network forensics Memory forensics Specialized tools Mac/Apple forensics Anti-forensic techniques Significance of time zones for analysis Anti-forensics/red team artifacts Time-stomping Case forensic activities Comprehensive Windows forensics simulated case Evidence report development Mock testimony

Lab Content

Students will work with remote lab environments to complete hands-on activities. MITRE ATTCK Matrix Analyze the Linux File System LoLBin SANS SIFT Decoding and Lolbins Network Forensics Memory Forensics Examining Windows Logs for Logon and Logoff Times Finding Users SIDS Advanced Memory Forensics Master File Table The Security Event Log Forensics Case Notes Ransomware Cloud Forensics Exploring Advanced Forensic Areas

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 the widely-accepted digital forensics frameworks. Read about multiple types of forensic analyses using Windows, Linux, and Macintosh-based tools. Read about digital forensics cases.

Writing Assignments

Complete a report of digital forensics analysis performed in preparation for expected expert witness testimony.

Out-of-class Assignments

Complete multiple types of forensics with Windows, Linux, and Macintosh-based tools. Complete hands-on lab to demonstrate and document proper digital forensics processes and procedures. Video an expert witness testimony. Conduct digital forensics analysis using tools resulting in a written report and expert witness testimony.

Demonstration of Critical Thinking

Students will conduct technical 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 forensics and incident handling tools and document the analysis performed in preparation for expert witness testimony.

Eligible Disciplines

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

years of professional experience, or any associate degree and six years of professional experience.

Textbooks Resources

1. Required Johansen, G. Digital Forensics and Incident Response, 3rd ed. Packt, 2022

Other Resources

1. Coastline Library 2. OER - Open Educational Resources