CYBR C256: MOBILE DEVICE FORENSICS

Item	Value
Curriculum Committee Approval Date	10/27/2023
Top Code	070800 - Computer Infrastructure and Support
Units	3 Total Units
Hours	68 Total Hours (Lecture Hours 54; Lab Hours 14)
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 mobile device forensic techniques using industry-recognized tools. Topics covered include an introduction to mobile forensics, investigative and extraction tools, cloud storage, device seizure, use of Faraday bags, and evidence reporting. 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: CYBR C150 and CYBR C230. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Evaluate a collection of digital evidence from mobile devices 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 related to mobile devices.
3. Given a simulated case, analyze the evidence of mobile devices and produce a report to describe evidence and present findings.

Course Objectives

- 1. Evaluate the digital forensics investigation lifecycle for mobile devices.
- 2. Demonstrate the use of industry-recognized tools to perform a forensic analysis of a simulated case for mobile devices.
- 3. Demonstrate the techniques used to find time-stomping and anti-forensic techniques for mobile devices.
- 4. Discuss the legal and ethical issues surrounding mobile device forensics, including privacy concerns and legal procedures.
- 5. Explore the architecture and components of mobile devices, including smartphones and tablets.
- 6. Demonstrate the use of tools and techniques for creating physical and logical images of mobile devices.
- 7. Describe how to recover and analyze various types of data from mobile devices, including text messages, call logs, photos, videos, and app data.

Lecture Content

Introduction to Mobile Forensics Stages of mobile forensics Stage 1 - device seizure Stage 2 - data acquisition Stage 3 - data analysis Acquisition Methods Overview Over-the-air acquisition Physical acquisition Mobile phone operating systems Acquisition - Android Devices Special considerations Wear leveling What happens to the deleted data. Acquisition and Introduction - iOs Generation of Apple hardware Acquisition methods overview Viewing and analyzing the image iOs - Logical and Cloud Acquisition Breaking backup passwords Decrypting the backup Mock testimony Dealing with Issues, Obstacles, and Special Cases Online versus offline authentication Unallocated space Encrypted storage SD card Mobile Forensic Tools and Case Studies

Lab Content

Students will work with remote lab environments to complete hands-on activities. Live data acquisition Cloud acquisition Comprehensive case analysis Anti-forensics Android/iOs mobile forensics

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 mobile forensics methodology. Read about multiple types of analyses using mobile forensics tools. Read about mobile forensics cases.

Writing Assignments

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

Out-of-class Assignments

Complete analysis with mobile forensics tools. Complete hands-on lab to demonstrate and document proper mobile forensics processes and procedures. Conduct mobile 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 tools and document the 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 Tamma, R.; Skulkin, O.; Mahalik, H.. Practical Mobile Forensics: Forensically investigate and analyze iOS, Android, and Windows 10 devices, 4th ed. Packt Publishing, 2020

Other Resources

1. Coastline Library 2. OER - Open Educational Resources