IT-2760: INTRODUCTION TO DIGITAL FORENSICS

Cuyahoga Community College

Viewing: IT-2760 : Introduction to Digital Forensics

Board of Trustees:

January 2021

Academic Term:

Fall 2021

Subject Code

IT - Information Technology

Course Number:

2760

Title:

Introduction to Digital Forensics

Catalog Description:

Introduction to Digital Forensics introduces the legal and technical aspects of digital forensics, including general forensic processes, imaging, hashing, file recovery, file system basics, identifying mismatched file types, reporting, and laws regarding computer evidence.

Credit Hour(s):

3

Lecture Hour(s):

2

Lab Hour(s):

2

Requisites

Prerequisite and Corequisite

ITNT-2380 Linux Administration.

Outcomes

Course Outcome(s):

Analyze digital data by applying appropriate forensic acquisition and processing methods.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Describe the standard digital forensic processes.
2. Create a forensic copy of a piece of digital media.
3. Verify a forensic copy.
4. Identify structures of file systems.
5. Recover deleted files.
6. Discuss laws related to computer evidence.

Methods of Evaluation:

Methods of evaluation can include:

1. Class participation and discussion
2. Oral and/or written reports
3. Homework assignments

4. Hands-on exercises/projects /labs
5. Quizzes
6. Examinations
7. Other methods deemed appropriate by the faculty

Course Content Outline:

1. Introduction to the digital forensics profession
    a. History of digital forensics
    b. Preparing for digital investigations
    c. Following legal processes
    d. Professional conduct
2. Data acquisition
    a. Understanding storage formats for digital evidence
    b. Determining the best acquisition method
    c. Using acquisition tools
3. Crime and incident scene processing
    a. Identifying digital evidence
    b. Collecting evidence
    c. Verify data integrity through the use of hash values
    d. Determining the tools you need
4. Forensics tools
    a. Types of digital forensics tools
    b. Tool comparisons
5. Working with operating systems and CLI
    a. The boot sequence
    b. Types of storage devices
    c. File structures
    d. Windows registry
6. Graphics file recovery
    a. Recognizing a graphics file
    b. Graphics file formats
    c. Tools for viewing images
    d. Steganography
7. Digital forensics analysis and validation
    a. Approaching digital forensics cases
    b. Validating forensic data
8. Current technology forensics
    a. Virtual machine forensics
    b. Email and social media
    c. Mobile device forensics
    d. Cloud forensics

Resources

Nelson, B., Phillips, A., & Steuart, C. *Guide to Computer Forensics and Investigations*. 6th. Boston: Cengage, 2019.

Easttom, C. *System Forensics, Investigation, and Response*. 3rd. Burlington: Jones and Bartlett, 2019.

Arnes, A. *Digital Forensics*. 1st. Hoboken: Wiley, 2017.

Top of page

Key: 4628