C-ID Descriptor
Digital Forensics Fundamentals

Descriptor Details

- **Descriptor Title**: Digital Forensics Fundamentals
- **C-ID Number**: 165
- **Units**: 3.0
- **Date of Last Revision**: 2/27/2025 09:51:02 AM PST

General Description

This course is an introduction to the methods used to properly conduct a computer forensics investigation beginning with a discussion of ethics, while mapping to the objectives of the International Association of Computer Investigative Specialists (IACIS) certification. Topics covered include an overview of computer forensics as a profession, the computer investigation process, understanding operating systems boot processes and disk structures, data acquisition and analysis, technical writing, and a review of familiar computer forensics tools.

Prerequisites

No information provided

Corequisites

No information provided

Advisories

ITIS 160 - Introduction to Information Systems Security

Each course content area should be supported with relevant hands-on exercises as much as possible.

Content

1. Computer Forensics as a profession
2. Computing investigation processes
3. Microsoft operating systems, boot processes and disk structures
4. Macintosh and Linux operating systems, boot processes and disk structures
5. The investigator’s office
6. Current computer forensics tools
7. Digital evidence controls
8. Crime/incident scene processing
9. Data acquisition
10. Computing forensics analysis
11. Email investigations
12. Graphic image recovery
13. High tech reports
14. Expert witness overview

Lab Activities

No information provided

Objectives

At the conclusion of this course, the student should be able to:

1. Define computer forensics.
2. Summarize how to prepare for a computer investigation.
3. Summarize the certification requirements for computer forensics labs.
4. Measure the different ways for proper data acquisition.
5. Classify the rules for proper digital evidence handling.
6. Analyze how data is stored and managed by an operating system.
7. Analyze various computer forensics tools.
8. Validate the evidence during the analysis process.
9. Identify and reconstruct graphics files.
10. Describe the importance of network forensics.
11. Analyze email investigations.
12. Generate a forensic report.

13. Describe guidelines for testifying in court.
14. Maintain a high level of ethical behavior in their work.

Evaluation Methods

Evaluation will include hands-on projects and a combination of examinations, presentations, discussions, or problem-solving assignments.

Textbooks

- Nelson, B. & Phillips, A., *Guide to Computer Forensics and Investigations*, Cengage
- Britz, M. T., *Computer Forensics and Cyber Crime: An Introduction*, Pearson