Digital Forensics in Cybersecurity – C840

Overview

Digital forensics, the science of investigating cybercrimes, seeks evidence that reveals who, what, when, where, and how threats compromise information. This course examines the relationships between incident categories, evidence handling, and incident management. Students identify consequences associated with cyber threats and security laws using a variety of tools to recognize and recover from unauthorized, malicious activities.

Competencies

- **Digital Evidence by Crime Category**
  The graduate identifies types of digital evidence, digital evidence examination rules, and digital evidence consideration by crime category.

- **Digital Forensics Procedures**
  The graduate describes digital forensics procedures from the initial recognition of an incident through the steps of evidence gathering, preservation, analysis, and through the completion of legal proceedings.

- **Laws, Rules, Policies, and Procedures**
  The graduate identifies laws, rules, policies, and procedures that affect digital forensics.

- **Forensics Evidence Analysis**
  The graduate conducts analysis on gathered evidence using forensic cyber tools to determine the nature of a security breach.

- **Recovery Procedures**
  The graduate executes recovery procedures for deleted data.

- **Steganography**
  The graduate identifies steganography and its techniques as it relates to concealed data.
Learning

Getting Started
Welcome to Digital Forensics in Cybersecurity. This course uses the uCertify learning resource which contains all of the necessary reading materials, interactive learning activities, knowledge checks, and labs. For the best understanding of the course content, complete each module assigned. To help you track your progress, we suggest you follow the pacing guide identified at the beginning of the course. Your competence will be demonstrated by the successful completion of an objective assessment and a performance assessment. Select the “Go to Course Materials” button to begin.

Assessments

Pre-Assessment: Digital Forensics in Cybersecurity
- STATUS: Not Attempted
- # OF ITEMS: 50
- TIME ALLOCATED: 150 minutes
- CODE: PHKO

Objective Assessment: Digital Forensics in Cybersecurity
- STATUS: Not Attempted
- # OF ITEMS: 50
- TIME ALLOCATED: 150 minutes
- CODE: HKO1
Status: **Not Attempted**  
Code: **HEP1**

A score of **Competent** or **Exemplary** is required to pass all assessments. Passing a preassessment does not guarantee you will pass the high stakes assessment.

On objective assessments, you will be charged a retake fee for the third attempt and every attempt thereafter. For more information [click here](#).

**Course Information**

- Accessibility Policy
- Student Success Center
- Example of a Search Warrant for Digital Evidence
- Forensics Methodology
- Seizing Electronic Evidence
- NIST Special Publication

**Course Instructor**

- **bscsia@wgu.edu**

**Announcements**
Course Search

Course Chatter