Advanced Digital Forensics

2023-2024 Catalog

[ARCHIVED CATALOG]

CSIA 235 - Advanced Digital Forensics

PREREQUISITES: SVAD 111 - Linux and Virtualization Tech and CSIA 105 - Introduction to Cyber Security/Information Assurance and ITSP 135 - Hardware / Software Support or (ITSP 132 - IT Support Essentials I and ITSP 134 - IT Support Essentials II).
PROGRAM: Cyber Security/Information Assurance
CREDIT HOURS MIN: 3
LECTURE HOURS MIN: 2
LAB HOURS MIN: 2
DATE OF LAST REVISION: Fall, 2020

Provides students with practical comprehension of the process and ethics within digital forensics and evidence analysis. Students will acquire hands-on experience with forensic investigation techniques and standard tools, Linux and Windows, necessary to successfully carry-out a digital investigation. This forensics course gives students the skills necessary to identify, track, and process evidence, excel in digital evidence acquisition/handling, forensic tools (PTK, FTK, Kali tools, and more) and lawful analysis in a forensically sound manner. Successful students of this course are able to approach a mock crime scene as a final exam and process it for a mock court of law as a case study milestone objective. The entire portfolio of the case such as, chain of custody forms, prelim analysis, notes, photos, forensics field kit tools used, and more, are the final submission, alon with a visual score of how and in what order the student processed the scene.

MAJOR COURSE LEARNING OBJECTIVES: Upon successful completion of this course the student will be expected to:

1. Identify the role of computer forensics in today's world.
2. Describe and identify the computer forensics investigation process from gathering the evidence through becoming an expert witness.
3. Describe and identify the search and seizure process.
4. Discuss digital evidence.
5. Identify First Responder procedures.
6. Discuss setup and design of computer forensics labs.
7. Analyze hard disks and file systems.
8. Analyze tools and techniques involved in Windows, Linux, Mac, and cloud forensics.
9. Implement data acquisition and duplication.
10. Recover deleted files and deleted partitions.
11. Utilize relevant software tools for forensics investigation management
12. Utilize relevant software tools for analyzing logs, events, images, network traffic, mobile devices and email.

COURSE CONTENT: Topical areas of study include -

- Software tools
- Forensic processes and procedures
- Crime investigation and reporting
- Incident response

- Hardware
- Digital forensics lab setup
- File system architecture
- Digital evidence, acquisition and storage
- Windows registry
- Legal procedures
- Data recovery
- Acquisition tools

Course Addendum - Syllabus (Click to expand)