Digital Forensics

2023-2024 Catalog

[ARCHIVED CATALOG]

CSIA 135 - Digital Forensics

PREREQUISITES: (ITSP 132 ITSP 132 - IT Support Essentials I and ITSP 134 ITSP 134 - IT Support Essentials II) or ITSP 135 ITSP 135 - Hardware / Software Support
PROGRAM: Cyber Security/Information Assurance
CREDIT HOURS MIN: 3
LECTURE HOURS MIN: 2
LAB HOURS MIN: 2
DATE OF LAST REVISION: Fall 2021

Provides students with an understanding of the detailed methodological approach to computer forensics and evidence analysis. Students will acquire hands-on experience with various forensic investigation techniques and standard tools necessary to successfully carry-out a computer forensic investigation.

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.
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 forensics.
9. Implement data acquisition and duplication.
10. Recover deleted files and deleted partitions.

11. Utilize relevant software tools for forensics investigations.

COURSE CONTENT: Topical areas of study include -

- Software tools
- Forensic processes
- Forensic procedures
- Incident response
- PC hardware
- File system architecture
- Digital evidence, acquisition and storage
- Windows registry
- Legal procedures
- Data recovery

GRADING POLICY

A.....90-100

B.....80-89

C.....70-79

D.....60-69

F.....0-59

Course Addendum - Syllabus (Click to expand)
