CIT 256: File System Forensic Analysis

This course discusses how data is stored on disk and where and how digital evidence can be found on the disk. The majority of digital evidence is found on a disk and knowing how and why the evidence exists can help an investigator to provide testimony in a more knowledgeable manner. Basic concepts and theory of a volume and file system are covered and applied to an investigation. The course also explores analysis techniques and special considerations that the investigator should make based on the file system. In addition, the data structures associated with volume and file systems are given and disk images are analyzed. The phases and guidelines of a digital investigation are also presented. Prerequisites: CIT 155 and CIS 106 and CIS 134, or permission of the instructor. Three hours of lecture per week. Instructional Support Fee applies. Gen. Ed. Competencies Met: Information Literacy.

Course Student Learning Outcomes

1. Understand digital investigation foundation.
2. Gain experience with different file systems.
3. Acquire a variety of analysis techniques.
4. Work with multiple operating systems and tools.
5. Learn how data is stored on computer persistent storage.
6. Practice finding digital evidence on computer disks.

Credits: 3
Program: Computer Information Technology