CIS 417 – Computer Forensics

Course Description

This course offers an introduction to system forensics investigation and response. Topics include procedures for investigating computer and cybercrime, tools, techniques, and methods used to perform forensic investigations and concepts for collecting, analyzing, recovering, and preserving forensic evidence.

Instructional Materials


Course Learning Outcomes

1. Identify the role of computer forensics in responding to crimes and solving business challenges.
2. Outline system forensics issues, laws, and skills.
3. Describe the purpose and structure of a digital forensics lab.
4. Examine and explain the evidence life cycle.
5. Identify the procurement of evidence in physical and virtualized environments.
6. Analyze the impact of sequestration on the evidence-gathering process.
7. Develop plans that collect evidence in network and email environments.
8. Examine automated digital forensic analysis.
9. Report investigative findings of potential evidentiary value.
10. Describe the constraints on digital forensic investigations.
11. Evaluate the ethical concerns that computer forensics issues raise in a global context.
12. Develop a computer forensics deployment plan that addresses and solves a proposed business problem.
13. Use technology and information resources to research issues in computer forensics.
14. Write clearly and concisely about computer forensics topics using proper writing mechanics and technical style conventions.