Undergraduate Certificate - Cybercrime Essentials

The undergraduate certificate in Cybercrime Essentials presents digital forensics tools and techniques used to detect, recognize, document, and verify cybercrime, cyber terrorism, cyberwarfare, cyberstalking, and cyberbullying. The rapid change in technology and the exponential growth in cybercrime means more skilled professionals are necessary to combat the effects of computer-related malice. This certificate program is intended for undergraduate students who seek to heighten their knowledge of cybercrime without committing to an academic degree program.

Coursework in this undergraduate certificate program aligns to the general objectives of the International Association of Computer Investigative Specialists (IACIS®) certification and meets the topical requirements for the Department of Defense Directive 8570.1M Information Assurance Management (IAM) Technical I, Technical II, Technical III, Management I, Management II, and Management III categories.

IACIS® is a registered trademark of the International Association of Computer Investigative Specialists, Inc.

Certificate Objectives

Upon successful completion of this certificate, the student will be able to:

- Appraise the rudiments of cybercrime and computer forensics. Profile the challenges of securing information on the Internet.
- Assess the process, the techniques, and technologies used by hackers to gain unauthorized access to information systems.
- Examine the processes, best practices, and techniques to manage and prevent cybercrime.
- Inspect the strategies and steps to investigate digital evidence in cybercrime. Construct the legal portfolio of digital evidence to support the prosecution of cybercrime.
- Examine the file structures, formats and technical protocols in storage subsystems encountered in gathering digital evidence.
- Develop a plan to analyze the processes and practices to seize and secure digital evidence at a crime scene and to collect evidence in both the private and public sectors.
- Analyze the steps and process used to identify, secure, catalog, and store digital evidence.

Certificate Requirements (18 semester hours)

Code	Title	Semester Hours
ISSC351	Computer Forensics	3
ISSC361	Information Assurance	3
ISSC422	Information Security	3
ISSC451	Cybercrime	3
ITMG371	Contemporary Internet Topics	3
ITMG281	Law, Privacy, and Digital Data	3
Total Semester Hours		18