Undergraduate Certificate - Digital Forensics

The undergraduate certificate in Digital Forensics examines various forensics models to identify, preserve, collect, analyze, prepare, and present evidence for prosecuting cybercrime. The window of opportunity for collecting evidence can be a few seconds or minutes depending on the sophistication of the perpetrator, and this program teaches the precise digital forensic measures needed to respond to security incidents to prevent loss or corruption of sensitive proprietary information. This certificate program is intended for undergraduate students who seek to heighten their knowledge of digital forensics without committing to an academic degree program.

Certificate Objectives

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

- Examine common incident response procedures via basic computer investigation processes and a good computer forensics lab for the development of investigative reports following first responder procedures.
- Investigate forensics of wireless network attacks, both caused by mobile and wireless peripheral devices, then evaluate security and access procedures within wireless Internet use subject search warrants and chain of custody in a forensic investigation.
- Explore web attacks, router forensics, e-mail tracking techniques, e-mail crime, and network forensics through investigation logs.
- Discuss corporate espionage and prevention techniques and computer-related crimes, such as sexual harassment and child pornography and the law.
- Analyze image files using forensic processes, recovered files on deleted partitions, data acquisition and duplication procedures, and steganography tools to create a forensic investigation case.
- Analyze file systems, hard disks, various types of digital media, tools, and applications that utilize password cracking on various operating systems.

Certificate Requirements (18 semester hours)

Code	Title	Semester Hours
ISSC351	Computer Forensics	3
ISSC455	Digital Forensics: Investigation Procedures and Response	3
ISSC456	Digital Forensics: Investigating Wireless Networks and Devices	3
ISSC457	Digital Forensics: Investigating Network Intrusions and Cybercrime Security	3
ISSC458	Digital Forensics: Investigating Data and Image Files	3
ISSC459	Digital Forensics: Hard Disc and Operating Systems	3
Total Semester Hours		18