



PROFESSIONAL CERTIFICATE IN **Digital Investigations**

Certificate Description

This certificate provides high school graduates, professionals with limited experience or out-of-field students and professionals the opportunity to understand the significance of digital investigation in today's business environment.

Introduction to Computer and Network Hardware—ITCO 103 (required)—This course provides the student with the knowledge about microcomputers and basic network hardware. Topics may include desktop and portable systems, printers, input devices, and fundamental networking components and concepts.

Outcomes:

- Describe various computing infrastructure components
- Configure computer and network resources
- Explain the operation of computers
- Discuss installation, maintenance, and configuration of computer and network hardware
- Explain the operation of key network hardware
- Explain the structure and function of the OSI model

Introduction to Operating Systems—ITCO 211 (required)—In this introduction to operating systems, students are exposed to contemporary desktop and mobile operating systems. Topics may include operating system support, functions, network requirements, virtualization, and basic maintenance.

Outcomes:

- Define the necessary components and functions of an operating system
- Explain steps to install a computer/network operating system
- Use command line utilities and scripting techniques for automating operating system tasks, including enterprise deployment
- Describe aspects of file systems for various operating systems
- Describe the benefits of integrating diverse operating systems within organizations
- Define the necessary components and functions of an operating system
- Explain steps to install a computer/network operating system
- Use command line utilities and scripting techniques for automating operating system tasks, including enterprise deployment
- Describe aspects of file systems for various operating systems
- Describe the benefits of integrating diverse operating systems within organizations



PROFESSIONAL CERTIFICATE IN **Digital Investigations**

Information Technology Security—ITCO 361 (required)—This survey course covers information security concepts and mechanisms. Information security concepts reviewed may include data protection techniques, software security, information assurance process, enterprise network security, and attack types/countermeasures.

Outcomes:

- Explain the fundamental concepts of information assurance and security.
- Discuss how operational issues such as software security and access management are addressed.
- Describe mechanisms for enterprise and Internet security.
- Discuss security management processes.
- Explain selected common security threats, vulnerabilities, and their countermeasures.

Introduction to Cyber Crime & Digital Investigation—ITDI 372—This course provides students with an introduction to the concepts and systems involved in digital investigations and cyber crime. The course discusses recognized incident response policies and procedures for collecting, preserving, analyzing, and reporting digital evidence, cyber crime history, and current and future threats.

Outcomes:

- Create professional technical reports
- Present report information appropriate for a client presentation or legal testimony
- Demonstrate appropriate use of technical information based on researched client knowledge level

Law & Ethics in Digital Investigations—ITDI 374—During this course, students will examine digital crime and investigation laws at various levels of government. Students will also discuss ethical concerns related to digital forensic investigations, and types of digital crime.

Outcomes:

- Identify and examine types of digital crime
- Describe ethical issues in digital investigations
- Discuss state, national, and international laws related to digital investigations
- Identify and analyze legal issues related to digital investigations



PROFESSIONAL CERTIFICATE IN **Digital Investigations**

Digital Investigations I—ITDI 375—This course will examine digital investigation tools, threats, and techniques. Topics may include procedures, steganography, operating systems, tool validation plans, and open source software.

Outcomes:

- Explain digital evidence collection procedures
- Demonstrate how to acquire digital evidence without causing alteration or damage to original data
- Analyze evidence from formatted media, deleted files, and unallocated space
- Develop reports for forensic evidence

Digital Investigations II—ITDI 379—During this course, students will examine digital investigation techniques for applications running for network operating systems.

Outcomes:

- Explain procedures for collection of digital evidence on networked systems
- Use advanced tools to analyze events in real-time
- Discuss issues related to live digital investigations

Network Investigations—ITDI 473—During this course, students will examine forensic techniques for collection, preservation, analysis, and reporting of digital network evidence. Topics may include network traffic analysis, electronic mail, and Internet investigations.

Outcomes:

- Explain the acquisition process for digital evidence from a network.
- Analyze digital evidence from a network
- Develop reports for forensic evidence.