Experience hands-on training in the industry standards for computer forensics investigation

Would you like to join an elite group of experts on the front lines of fighting cybercrime? With the evolution of technology and significant increases in computer-based crimes, the field of computer forensics is one of the fastest growing disciplines in computer security. As crimes become more technologically sophisticated, the need for computer forensic experts will continue to grow throughout law enforcement and the business community.

Get the training you need to start a career in this exciting and challenging field. You will get hands-on experience using Encase – the industry standard in computer forensic investigation technology – and Forensic Toolkit (FTK) – a suite of technologies used to perform forensic examinations of computer systems. You will also learn how to image different devices.

The online Certificate in Computer Forensics provides a great opportunity to develop the skills and expertise you need to succeed.

The program includes five online courses totaling 92 hours of lecture and hands-on experience. The certificate graduate will receive 9.2 Continuing Education Units (CEUs), a nationally recognized unit used for professional development.

Who Should Attend?
- Information technology specialists
- Systems analysts
- Network administrators
- Computer forensics professionals

Eligibility
The Certificate in Computer Forensics is appropriate for people who want to expand their expertise and learn the essential components intrinsic to the field of computer forensics. The core audience includes individuals working in public or private corporations and government entities, as well as legal and law enforcement organizations.
Certificate in
COMPUTER FORENSICS I

THE CLASSES

Introduction to Computer Forensic Methodology
(1.6 CEUs/16 hours)
Prerequisite: a working knowledge of basic IT concepts and networking experience is recommended. This class provides an overview of the history of computer forensics in the evolution of cyber-crimes. Individuals will gain a basic understanding and legal awareness of computer forensics, the techniques used in the evidentiary process, the various methodologies intrinsic to computer forensics with an emphasis on computer incident response and evidence gathering and processing methodologies. The importance of ethics, understanding rules of evidence, effective communications, key elements of search and seizure relative to privacy legislation will also be discussed.

Forensic Evidence Preservation
(0.8 CEUs/8 hours)
Prerequisite: Introduction to Computer Forensics Methodology or permission of program manager. This class focuses on basic concepts of properly preserving computer, or digital media evidence. Individuals will learn the preparation process associated with imaging and storing electronic evidence, how to forensically preview computer media, and the operations of imaging devices such as Forensic Toolkit (FTK) Imager, Encase and Partition Dump (DD). Individuals will gain an understanding of how to verify the integrity of an image file.

Class includes a Digital Intelligence ULTRABLOCK-USB Kit for students to keep

Tools & Technology of Computer Forensic Investigations
(3 CEUs/30 hours)
Prerequisite: Forensic Evidence Preservation or permission of program manager. This class will examine the common tools employed in conducting a computer forensic investigation. The focus of the class is to bestow a working knowledge of the Forensic Toolkit (FTK) and Encase tools. Individuals will learn to apply the appropriate forensic tools through hands-on experience using real-world scenarios.

Forensic Evidence Analysis
(3 CEUs/30 hours)
Prerequisite: Tools & Technology of Computer Forensic Investigations or permission of program manager. This class is an in-depth study into evidence analysis of computer forensic investigations and the challenges of incident response analysis. Individuals will learn to identify, replicate and analyze digital data prior to corruption in evaluating containment of a potential compromise. Focus will be on the investigative aspects relative to the legal integrity of the data analysis. Individuals will adhere to the laws of evidence in collecting, preserving, analyzing, and presenting computer forensics evidence in legal proceedings.

Computer Forensics – Investigative Simulation
(0.8 CEUs/8 hours)
Prerequisite: completion of the four previous classes in this certificate program. This capstone class is conducted in a laboratory environment that provides hands-on experience using software to create a live simulation of compromised system images to demonstrate the components inherent in forensic investigations. You will learn to identify and analyze digital data and to appropriately present the findings as evidence in litigation proceedings.

Register today at extension.fullerton.edu/professionaldevelopment or 657.278.2611
For more information, contact Veronica Martinez: 657.278.3123, vmartinez@fullerton.edu
University Extended Education

extension.fullerton.edu/professionaldevelopment