When it comes to technology, today’s next big thing is tomorrow’s antique. Cyber criminals are almost always ahead of the trends, and our program follows suit by always evolving to help you keep up with the latest advances in computer forensics. To help you get to the forefront of the field – and stay there – as quickly as possible, we combine the convenience and efficiency of a fully online course with the invaluable hands-on experience of working with the latest tools in the field.

Our sequential curriculum starts with basic methodology and finishes with an immersive capstone class that will simulate a live investigation where you’ll use the methods and tools covered during the program. It all culminates in a mock trial, where you’ll get the chance to put everything you’ve learned to the test as you take the stand and present your evidence as an expert witness.

We keep pace with the latest technology – so you can too
1. Introduction to Computer Forensic Methodology

This class provides an overview of the history of computer forensics and the evolution of cyber-crimes. You 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.

2. Forensic Evidence Preservation

This class focuses on basic concepts of properly preserving computer, or digital media evidence. You will learn 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).

3. Tools & Technology of Computer Forensic Investigations

Examine the common tools employed in a computer forensic investigation. The focus of the class is to develop a working knowledge of the Forensic Toolkit (FTK) and EnCase tools. You will learn to apply the appropriate forensic tools through hands-on experience using real-world scenarios.

4. Forensic Evidence Analysis

This class is an in-depth study in evidence analysis of computer forensic investigations and the challenges of incident response analysis. You will learn to identify, replicate and analyze digital data prior to corruption in evaluating containment of a potential compromise.

5. Computer Forensics - Investigative Simulation

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.