Certified Digital Forensics Examiner

5 Days

Introduction

This course will benefit companies, organizations, individuals and government security agencies intent on pursuing any corrective action, litigation or proof of guilt based on digital evidence.

A case in point could be the termination of an employee for a violation that may involve a digital artifact to support the allegation. The investigator must furnish irrefutable burden of proof derived from the digital artifact. If not, then an attorney who is knowledgeable about Computer Forensics would have the case thrown out. Similarly, Government or investigative agencies need to be able to successfully prosecute or defend cases such as acts of fraud, computer misuse, illegal pornography or counterfeiting and so forth.

Course Outline

Computer Forensics was developed by U.S. federal law enforcement agents during the mid to late 1980s to meet the challenges of white-collar crimes being committed with the assistance of a PC. By 1985 enforcement agents were being trained in the automated environment and by 1989 software and protocols were beginning to emerge in the discipline.
The Certified Digital Forensics Examiner program is designed to train Cyber Crime and Fraud Investigators whereby students are taught electronic discovery and advanced investigation techniques. This course is essential to anyone encountering digital evidence while conducting an investigation.

Upon Completion

Certified Digital Forensics Examiner graduates will obtain real world computer forensic knowledge that will help them recognize, seize, preserve and present digital evidence. Graduates will be able to confidently attempt the Forensics certification:
Certified Digital Forensics Examiner (CDFE)