EC-Council

PROGRAM BROCHURE

C|F F™
Computer Forensics Fundamentals

Computer Forensics Fundamentals

C|F F™
Computer Forensics Fundamentals

The Critical Nature of Computer Forensic

The rapid evolution of computers has brought technical devices as an active weapon to criminals. Cybercriminals have enjoyed the pleasure of being able to combine a large array of complex technologies to be successful in their mission. Due to the complexity of the attack, investigating a crime in the cyber world has become increasingly difficult to do.

Computer forensics is used in different types of investigations like crime and civil investigation, corporate litigation, cybercrime etc. It plays a vital role in the investigation and prosecution of cybercriminals. It refers to a set of methodological procedures and techniques to identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment so that the discovered evidence can be used during a legal and/or administrative proceeding in a court of law.

Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud.

Course Description

Computer Forensics Fundamentals (C|FF) is an entry-level security program covering the fundamental concepts of information security. Through this program, students can build skills to identify information security threats which reflect on the security posture of the organization and implement general security controls.

This program gives a holistic overview of the key components of computer forensics. It provides a solid fundamental knowledge required for a career in computer forensics.

The Computer Forensics Fundamentals course significantly benefits students interested in learning the fundamentals of computer forensics.

Why C|FF Is Important

- It facilitates your entry into the world of computer forensics
- It provides a professional understanding of the concepts of computer forensics
- It enhances your skills as a Computer Forensics Specialist and increases your employability

C|F F™
Computer Forensics Fundamentals

Target Audience

The Computer Forensics Fundamentals course is designed for anyone looking to enhance their skills and build a career in information security and computer forensics.

Suggested Course Duration:

2 Days I 16 hours total class time

Certification

Post the completion of attending the complete official course, candidates will receive their Certificate of Attendance.

Course Outline

Module 01: Computer Forensics Fundamentals

Module 02: Incident Response and Forensics

Module 03: Digital Evidence

Module 04: Understanding Hard Disks and File Systems

Module 05: Windows Forensics

Module 06: Network Forensics and Investigating Network Traffic

Module 07: Steganography

Module 08: Analyzing Logs

Module 09: E-mail Crime and Computer Forensics

Module 10: Introduction to Writing Investigative Report

Learning Objectives of the C|FF Program

- Understanding the key issues plaguing the computer forensics
- Learn the trademark, copyright, and patents
- Master the incident handling and response process
- Master cyber-crime and computer forensics investigation methodology
- Understand the different types of digital evidence and digital evidence examination process
- Understand the different types of file systems and their comparison (based on limit and features)
- Learn to gather volatile and non-volatile information from Windows and network forensics analysis mechanism
- Understand steganography and its techniques
- Gain an understanding of the different types of log capturing, time synchronization, and log capturing tools
- Master the art of e-mail tracking and e-mail crime investigation
- Learn to write an investigation report

C|FF™
Computer Forensics Fundamentals

EC-Council