



Computer Hacking Forensic Investigator (CHFI) Exam Prep

UWF Florida Cybersecurity Training Program
Offered by the University of West Florida Center for Cybersecurity

Course Overview

Course / Cyber Skills Exercise Dates: October 7 - December 6, 2024

Duration: 8 weeks + exam week

Estimated Time Commitment: 20 hours per week

Instructional Hours: 40 contact hours

Delivery Format: Asynchronous online with weekly optional zoom help sessions

Target Audience: IT and Cybersecurity practitioners with experience as an analyst, administrator, auditor, or similar position in an area of cybersecurity.

Required Prerequisites / Background: A minimum of 2 years IT security experience

CEUs: 4, **CPEs:** 48

Course Instructor(s):

Instructor	Email
Elizabeth Rasnick	erasnick@uwf.edu
Hossain Shahriar	hshahriar@uwf.edu

Course Description

This course uses the EC Council exam preparation resources to equip learners with the knowledge and skills needed to sit for the Computer Hacking Forensic Investigator (CHFI) certification exam. The course contains 15 learning modules.

EC Council’s course description:

This class is designed to provide the participants with the necessary skills to perform an effective digital forensics investigation. The course presents a methodological approach to computer forensics, including searching and seizing, chain-of-custody, acquisition, preservation, analysis, and reporting of digital evidence. It is a comprehensive course covering major forensic investigation scenarios that enables students to acquire the necessary hands-on experience on various forensic investigation techniques and standard forensic tools necessary to successfully carry out a computer forensic investigation leading to the prosecution of perpetrators.





Module 01 - Computer Forensics in Today's World	Module 09 - Malware Forensics
Module 02 - Computer Forensics Investigation Process	Module 10 - Investigating Web Attacks
Module 03 - Understanding Hard Disks and File Systems	Module 11 - Dark Web Forensics
Module 04 - Data Acquisition and Duplication	Module 12 - Cloud Forensics
Module 05 - Defeating Anti-forensics Techniques	Module 13 - Email and Social Media Forensics
Module 07 - Linux and Mac Forensics	Module 14 - Mobile Forensics
Module 06 - Windows Forensics	Module 15 - IoT Forensics
Module 08 - Network Forensics	Certification Exam

NIST NICE Cybersecurity Workforce Framework Mapping

The course prepares for the following cybersecurity work roles as defined by the NICE Cybersecurity Workforce Framework.

Cybersecurity Work Roles and Categories:

- Systems Security Analyst (Operate and Maintain)
- Cyber Defense Analyst (Protect and Defend)
- Vulnerability Assessment Analyst (Protect and Defend)
- Information Systems Security Manager (Oversee and Govern)
- Warning Analyst (Analyze)