Computer Hacking Forensic Investigator

Course Duration: 40 Hrs. **Course code: CHFIv11**

Course Overview

The Computer Hacking Forensic Investigator (CHFI) course equips individuals with the knowledge and skills to conduct effective digital forensics investigations, focusing on detecting hacking attacks, gathering evidence, and analyzing data for cybercrime prevention.

What you'll learn?

- **Digital Evidence Acquisition and Handling:**
  Learn to collect, preserve, and manage digital evidence from various sources, including computers, networks, and mobile devices.
- **Forensic Analysis:**
  Develop the ability to analyze digital evidence to determine the nature and scope of a security incident, identify the root cause, and reconstruct events.
- **Chain of Custody:**
  Understand the importance of maintaining a secure and verifiable chain of custody for digital evidence to ensure its admissibility in court.
- **Legal Procedures:**
  Gain knowledge of relevant laws and regulations related to digital forensics and cybercrime investigations.

Target Audience

The target audience for a Computer Hacking Forensic Investigator (CHFI) program or certification includes IT professionals involved in information system security, computer forensics, and incident response, including law enforcement, government agencies, and cybersecurity professionals.

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

Pre-Requisites

- **Basic IT/Cybersecurity Knowledge:**
  Understanding of basic cybersecurity concepts, such as firewalls, antivirus, and basic network security practices is essential.
- **Familiarity with Incident Response:**
  Basic knowledge of incident response processes and procedures is crucial.
- **Understanding of Computer Forensics:**
  A foundational understanding of computer forensics principles and techniques is necessary.
- **Knowledge of Cybercrimes and Investigation Procedures:**
  Understanding cybercrimes and their investigation procedures is vital.

Course content

Module 01: Computer Forensics in Today's World

A. Understand the Fundamentals of Computer Forensics
B. Understand Cybercrimes and their Investigation Procedures
C. Understand Digital Evidence and eDiscovery.
D. Understand Forensic Readiness
E. Understand the Role of Various Processes and Technologies in Computer Forensics
F. Identify the Roles and Responsibilities of a Forensic Investigator
G. Understand the Challenges Faced in Investigating Cybercrimes
H. Understand Various Standards and Best Practices Related to Computer Forensics
I. Understand Laws and Legal Compliance in Computer Forensics

Module 02: Computer Forensics Investigation Process

A. Understand the Forensic Investigation Process and its Importance.
B. Understand First Response
C. Understand the Pre-investigation Phase.
D. Understand the Investigation Phase
E. Understand the post-investigation Phase.

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

Module 03: Understanding Hard Disks and File Systems

A. Describe Different Types of Disk Drives and their Characteristics.
B. Explain the Logical Structure of a Disk
C. Understand the Booting Process of Windows, Linux, and macOS Operating Systems
D. Understand Various File Systems of Windows, Linux and macOS Operating Systems
E. Understand File System Analysis
F. Understand Storage Systems
G. Understand Encoding Standards and Hex Editors
H. Analyze Popular File Formats Using Hex Editor

Module 04: Data Acquisition and Duplication

A. Understand Data Acquisition Fundamentals
B. Understand eDiscovery.
C. Understand Data Acquisition Methodology
D. Prepare an Image File for Examination

Module 05: Defeating Anti-forensics Techniques.

A. Understand Anti-forensics Techniques.
B. Discuss Data Deletion and Recycle Bin Forensics
C. Illustrate File Carving Techniques and Ways to Recover Evidence from Deleted Partitions
D. Explore Password Cracking/Bypassing Techniques
E. Detect Steganography, Hidden Data in File System Structures, Trail Obfuscation, and File Extension Mismatch
F. Understand Techniques of Artifact Wiping, Overwritten Data/Metadata Detection, and Encryption
G. Detect Program Packers and Footprint Minimizing Techniques

Module 06: Windows Forensics

A. Understand Windows Forensics

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

B. Collect Volatile Information
C. Collect Non-volatile Information
D. Perform Windows Memory Analysis
E. Perform Windows Registry Analysis
F. Perform Electron Application Analysis
G. Perform Web Browser Forensics
H. Examine Windows Files and Metadata
I. Understand ShellBags, LNK Files, and Jump Lists
J. Understand Text-based Logs and Windows Event Logs

Module 07: Linux and Mac Forensics

A. Collect Volatile Information in Linux
B. Collect Non-volatile Information in Linux
C. Understand Linux Memory Forensics
D. Understand Mac Forensics
E. Collect Volatile Information in Mac
F. Collect Non-volatile Information in Mac
G. Understand Mac Memory Forensics and Mac Forensics Tools

Module 08: Network Forensics

A. Understand Network Forensics
B. Summarize Event Correlation Concepts
C. Identify Indicators of Compromise (IoCs) from Network Logs
D. Investigate Network Traffic
E. Perform Incident Detection and Examination Using SIEM Tools
F. Understand Wireless Network Forensics
G. Detect and Investigate Wireless Network Attacks

Module 09: Malware Forensics

A. Understand Malware Concepts
B. Understand Malware Forensics
C. Perform Static Malware Analysis
D. Analyzing Suspicious Documents

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

E. Perform System Behavior Analysis
F. Perform Network Behavior Analysis
G. Perform Ransomware Analysis

Module 10: Investigating Web Attacks

A. Understand Web Application Forensics
B. Understand Internet Information Services (IIS) Logs
C. Understand Apache Web Server Logs
D. Detect and Investigate Various Attacks on Web Applications

Module 11: Dark Web Forensics

A. Understand the Dark Web and Dark Web Forensics
B. Determine How to Identify the Traces of Tor Browser during Investigation
C. Perform Tor Browser Forensics

Module 12: Cloud Forensics

A. Understand Cloud Computing Concepts
B. Understand Cloud Forensics
C. Understand Amazon Web Services (AWS) Fundamentals
D. Perform AWS Forensics
E. Understand Microsoft Azure Fundamentals
F. Perform Microsoft Azure Forensics
G. Understand Google Cloud Fundamentals
H. Perform Google Cloud Forensics

Module 13: Email and Social Media Forensics

A. Understand Email Basics
B. Explain Email Crime Investigation and its Steps.
C. Understand U.S. Laws Against Email Crime
D. Explain Social Media Forensics

Module 14: Mobile Forensics

A. Understand Mobile Device Forensics

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

B. Understand Android and iOS Architecture, Boot Process, and File Systems
C. Understand Mobile Forensics Process
D. Investigate Cellular Network Data
E. Perform File System Acquisition
F. Understand Phone Locks, Rooting, and Jailbreaking of Mobile Devices
G. Perform Logical Acquisition on Mobile Devices
H. Perform Physical Acquisition on Mobile Devices
I. Perform Android and iOS Forensic Analysis

Module 15: IoT Forensics

A. Understand IoT Concepts
B. Perform Forensics on IoT Devices

Exam Preference

Exam Code	312-49
Length Of Test	240 Minutes
Number Of Questions	150 MCQ.
Passing Score	60%-85%