



Cyber Security / Digital Forensics

Course Introduction:

In an age where cyber threats are increasingly sophisticated and pervasive, understanding digital forensics is crucial for organizations seeking to protect their assets and respond effectively to security incidents. This 5-day training course, "Cyber Security | Digital Forensics," is designed to provide participants with a comprehensive overview of digital forensics principles, methodologies, and tools. Attendees will learn how to investigate cyber incidents, analyze digital evidence, and apply forensic techniques to uncover the truth behind security breaches.

Throughout the course, participants will explore key concepts in digital forensics, including data recovery, evidence collection, and legal considerations. By examining real-world case studies and engaging in discussions about emerging threats, attendees will gain practical insights into the role of digital forensics in cybersecurity. This course aims to equip professionals with the skills necessary to conduct thorough investigations and contribute to their organization's overall security posture.

Course Objectives:

By the end of the program, participants will be able to:

- Understand the fundamentals of digital forensics and its significance in cybersecurity.
- Learn key methodologies and tools used in digital forensic investigations.
- Explore the process of evidence collection, preservation, and analysis.
- Analyze legal and ethical considerations in digital forensics.
- Develop skills for reporting findings and presenting evidence in a clear manner.

Who Should Attend?

This course is intended for Cybersecurity professionals and analysts, IT security personnel involved in incident response, Law enforcement and legal professionals and IT auditors and compliance officers.

Course Outline:

Day 1: Introduction to Digital Forensics

- Overview of digital forensics and its role in cybersecurity
- Key concepts and terminology in digital forensics
- The digital forensics lifecycle: from incident detection to reporting

Day 2: Forensic Methodologies and Tools

- Exploring various digital forensic methodologies
- Overview of popular forensic tools and software
- Understanding the importance of chain of custody in evidence handling

Day 3: Evidence Collection and Preservation

- Techniques for collecting digital evidence from various devices
- Best practices for preserving data integrity during investigations
- Analyzing different types of digital evidence (e.g., hard drives, networks)

Day 4: Analysis and Interpretation of Forensic Evidence

- Methods for analyzing digital evidence and identifying anomalies
- Understanding file systems, data structures, and recovery techniques
- Case studies on successful forensic investigations

Day 5: Legal and Ethical Considerations in Digital Forensics

- Overview of relevant laws and regulations in digital forensics
- Ethical dilemmas and responsibilities of forensic investigators
- Communicating findings: reporting and presenting evidence effectively

Course Methodology:

A variety of methodologies will be used during the course that includes:

- (30%) Based on Case Studies
- (30%) Techniques
- (30%) Role Play
- (10%) Concepts
- Pre-test and Post-test
- Variety of Learning Methods
- Lectures
- Case Studies and Self Questionnaires
- Group Work

Course Fees:

To be advice as per course location. This rate includes participant's manual, Hands-Outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Certificate:

International Center for Training & Development (ICTD) will award an internationally recognized certificate(s) for each delegate on completion of training.

Course Timings:

Daily Course Timings:

08:00 - 08:20	Morning Coffee / Tea
08:20 - 10:00	First Session
10:00 - 10:20	Coffee / Tea / Snacks
10:20 - 12:20	Second Session
12:20 - 13:30	Lunch Break & Prayer Break
13:30 - 15:00	Last Session