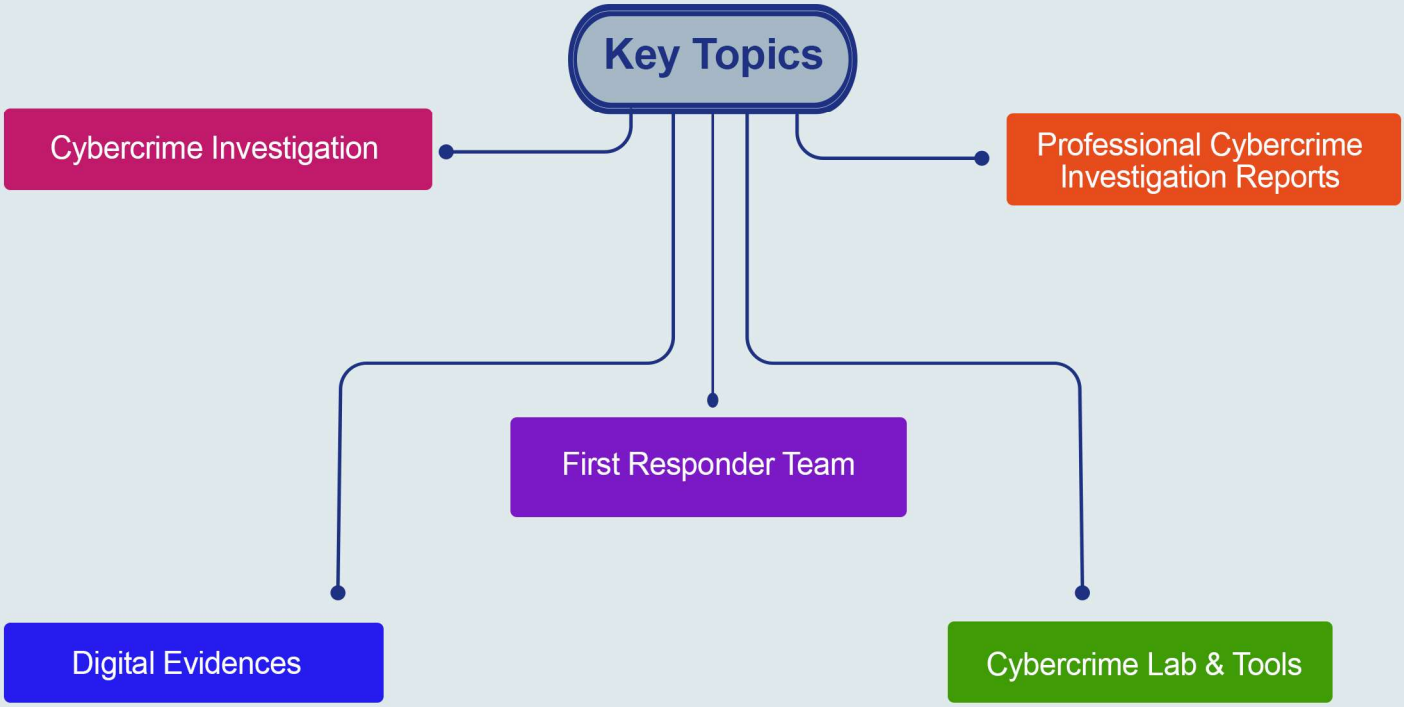
About the Course

The field of Digital Forensics is all about retrieving digital data from a wide range of digital and computer devices. The most obvious reason that this data would need to be identified and extracted is to be used as evidence in some sort of case related to computer crime. In this course you learn the Digital Forensics essentials and the necessary knowledge to understand the Digital Forensics disciplines, how to be an effective and efficient Digital Forensics practitioner, and how to effectively use digital evidence.

Learning Objectives

1. Understanding Digital Forensics Concepts
2. Understanding Digital Evidence
3. How Digital Forensics Can Assist Organizations or Investigation
4. Digital Forensics Principles and Processes
5. Manage Incident Response Processes and Procedures
6. Build and Maintain a Digital Forensics Capacity

Key Topics



Pre Requisites

- Information Security Incident Management Course

Terminus System

What You Will Receive

- Course Presentation File
- Complementary Files
- Cybersecurity Forensics eBook

Who Should Attend

Attend this course if you are responsible for information security incidents forensics. This course is for:

- Cyber Forensics Analysts
- Cyber Intelligence Specialist

Terminus System

Syllabus

Cybercrime Forensics

- Evolution of Computer Forensics Science
- Objective of Computer Forensics
- Need for Compute Forensics and Computer Forensics and Investigation
- Types of Cybercrimes
- How to Investigate Cybercrimes

Computer Forensics Investigation Process

- Investigating Computer Crime
- Steps to Prepare for a Computer Forensics Investigation
- Computer Forensics Investigation Methodology

Searching & Seizing Computers

- Searching and Seizing Computers without a Warrant
- Searching and Seizing Computers with a Warrant
- The Electronic Communications Privacy Act
- Electronic Surveillance in Communications Networks
- Evidence

Digital Evidences

- Digital Data
- Types of Digital Data
- Electronic Devices: Types and Collecting Potential Evidence
- Identifying Digital Evidence
- Digital Evidence Examination Process
- Evidence Admissibility
- Rules of Evidence
- Daubert Standard

Syllabus

First Responder Procedures

- Electronic Evidence
- First Responder
- Roles of First Responder
- Electronic Devices: Types and Collecting Potential Evidence
- First Responder Toolkit
- First Response Basics
- Securing and Evaluating Electronic Crime Scene
- Conducting Preliminary Interviews
- Documenting Electronic Crime Scene
- Collecting and Preserving Electronic Evidence
- Packaging and Transporting Electronic Evidence
- Reporting the Crime Scene
- Note Taking Checklist

Cybercrime Forensics Laboratory

- Establish a Cybercrime Forensics Laboratory
- Investigative Services in Computer Forensics
- Cybercrimes Forensics Hardware
- Cybercrimes Forensics Software

Preparing Investigative Reports

- Computer Forensics Report
- Computer Forensics Report Template
- Investigative Report Writing
- Sample Forensics Report

Syllabus

Expert Witness

- Who is an Expert Witness?
- Types of Expert Witnesses
- Scope of Expert Witness Testimony
- Evidence Processing
- Rules for Expert Witness
- Finding a Computer Forensic Expert

Hands-on Training

- Lab 1: Forensic Examination of Digital Evidence
- Lab 2: Collecting Evidence from a Running Computer
- Lab 3: Forensic Replicator
- Lab 4: Hard Disks and File Systems