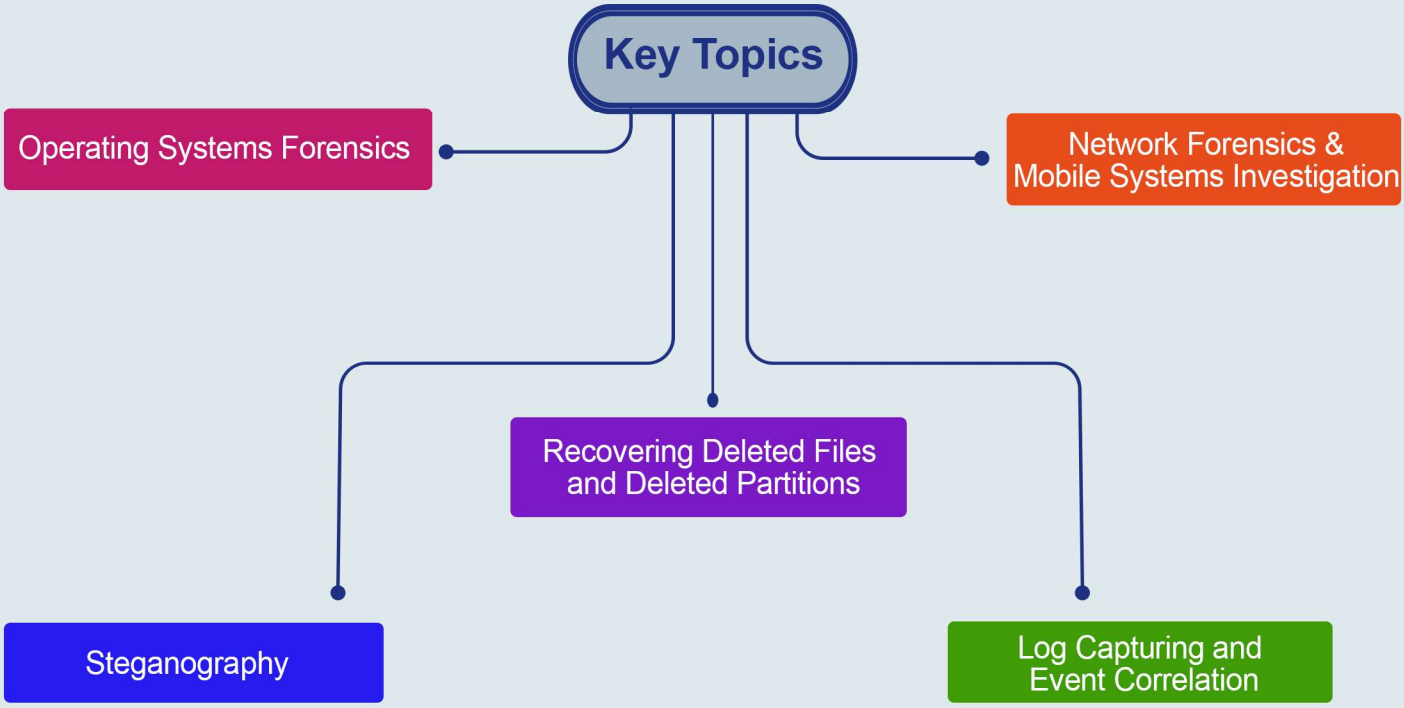
About the Course

Digital forensics involves the investigation of computer-related crimes with the goal of obtaining evidence to be presented in a court of law. In this course, you will learn the principles and techniques for digital forensics investigation and the spectrum of available computer forensics tools. You will learn about core forensics procedures to ensure court admissibility of evidence, as well as the legal and ethical implications. You will learn how to develop your practical and professional skills in digital forensics. The course aims to explain the scientific principles and techniques behind the work of forensic scientists.

Learning Objectives

1. Perform a forensic investigation on both Unix/Linux and Windows systems with different file systems
2. Manage forensic procedures and review and analyze forensics reports
3. Do court admissibility investigative procedures
4. Investigate Windows and Unix/Linux file systems and file recovery processes
5. Identify and apply appropriate forensics tools to acquire, preserve & analyze system image
6. Review and critique a forensics report

Key Topics



Pre Requisites

- Cyber Security Forensics - Preliminary 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
- Incident Responders

Syllabus

Understanding Hard Disks and File Systems

- Hard Disk Drive Overview
- Disk Partitions and Boot Process
- Understanding File Systems

Windows Forensics

- Collecting Volatile Information
- Collecting Non-volatile Information
- Examine File Systems
- Examine Memory
- Windows Registry Analysis
- Cache, Cookie, and History Analysis
- MD5 Calculation
- Windows File Analysis
- Metadata Investigation
- Other Audit Events
- Forensic Analysis of Event Logs
- Windows Password Issues
- Forensic Tools

Data Acquisition and Duplication

- Data Acquisition and Duplication Concepts
- Data Acquisition Types
- Disk Acquisition Tool Requirements
- Validation Methods
- RAID Data Acquisition
- Acquisition Best Practices
- Data Acquisition Software Tools
- Data Acquisition Hardware Tools

Syllabus

Recovering Deleted Files and Deleted Partitions

- Recovering the Deleted Files
- File Recovery Tools for Windows
- File Recovery Tools for MAC
- File Recovery Tools for Linux
- Recovering the Deleted Partitions
- Partition Recovery Tools
- TestDisk for Linux

AccessData FTK Toolbox

- Specifications
- How to install
- Configuration
- Interface
- Decrypting EFS and other Encrypted Files
- Working with Reports
- Viewing and Distributing a Report

Encase Toolbox

- Overview of EnCase Forensic
- Installing EnCase Forensic
- EnCase Interface
- Case Management
- Working with Evidence
- Adding a Device using Tableau Write Blocker
- Source Processor
- Creating an Analysis Job
- Viewing File Content
- Bookmarking Items
- Reporting

Syllabus

Image Files Forensics and Steganography

- What is Steganography?
- Steganography Techniques
- Steganography Tool
- Image file identification and retrieval tool
- Data Compression
- Locating and Recovering Image Files
- Image File Forensics Tools
- Universal Viewer

Application Password Cracking

- Password Cracking Concepts
- Types of Password Attacks
- Classification of password cracking tools
- Types of password cracking tools
- Bypassing BIOS Passwords
- Application Software Password Cracking
- Password Cracking Tools

Log Capturing and Event Correlation

- Computer Security Logs
- Logs and Legal Issues
- Log Management
- Centralized Logging and Syslogs
- Time Synchronization
- Event Correlation
- Log Capturing and Analysis Tools

Syllabus

Network Forensics

- Network Forensics
- Network Attacks
- Investigating Network Traffic
- Traffic Capturing and Analysis Tools
- Documenting the Evidence Gathered on a Network

Wireless Systems Forensics

- Wireless Technologies
- Wireless Attacks
- Investigating Wireless Attacks
- Features of a Good Wireless Forensics Tool
- Wireless Forensics Tools

Investigating Web Attacks

- Introduction to Web Applications and Webservers
- Web Logs
- Web Attacks
- Web Attack Detection Tools

Investigating e-mail crimes

- Email System Basics
- Email Crimes
- Email Header
- Steps to Investigate
- Email Forensics Tools

Syllabus

Mobile Systems Investigation

- Mobile Phone
- Mobile Operating Systems
- Mobile Forensics
- Mobile Forensic Process
- Mobile Forensics Software Tools
- Mobile Forensics Hardware Tools

Digital Forensics for Linux/Unix

- Tools Throughout
- Forensic Preparation and Best Practices
- Vital Investigation Tools
- Taking a Live System Snapshot
- Creating Bit Images
- Media Analysis
- File System Basics
- MAC Times and Timeline Analysis
- Recovering Deleted Files
- Searching Unallocated Space
- String Searches
- Incident Reporting

Hands-on Training

- Lab 1: Windows Forensics
- Lab 2: Data Acquisition and Duplication
- Lab 3: Recovering Deleted Files and Partition
- Lab 4: Forensics Investigations Tools
- Lab 5: Steganography
- Lab 6: Application Password Crackers