Digital Forensics Expert

www.us-council.com

This course is mapped to Digital Forensics Expert (DFE) Certification Exam from US-Council.

Training can be taken from anywhere in the world through our Authorized Training Partners or through Online Training offering at the link below:

http://us-council.com/training.php

This course is designed for experienced security professionals and deals with the theory and practice of digital forensics. It covers a wide range of topics all the way from basic disk forensics to smartphone and mobile forensics. This course will equip cyber investigators with the right skills and tools to perform a complete digital forensic analysis and investigation.

Introduction to Cybercrime

- Introduction
- What is Cyber Forensics
- Understanding the Science of Forensics
- Classifications of Cybercrimes
    - E-Mail Spoofing
    - Cyber defamation
    - Data Diddling
    - Industrial Espionage
    - Hacking
    - Online Frauds
    - Pornographic Offenses
    - Software Piracy
    - Computer Sabotage
    - E-Mail Bombing
    - Computer Network Instructions
    - Password Sniffing
    - Identity Theft

- Cybercrime: The Legal Perspectives
- Cybercrime: An Indian Perspective
- Cybercrime and Information Security
- Cybercrime and the Indian ITA 2000
    - Hacking and the Indian Law(s)

Careers in CyberForensics

- Introduction
- IT Security Organization
- Roles and Responsibilities
- Career paths in Cybersecurity
    - Assurance and Compliance Security Audit
    - Types of Assurance and Compliance
    - Network Security
    - Cybercrime Investigation and Litigation
    - Computer Forensics

- Cybersecurity Certifications

Cybercrimes and the CyberSecurity: The Legal Perspectives

- Introduction
- Cybercrime and the Legal Landscape around the World
    - Online Safety and Cybercrime Laws
    - Cybercrime Law Scenario in the Asia-Pacific Region
    - Cybercrime and Federal Laws in the US
    - The EU Legal Framework for Information Privacy to Prevent Cybercrime
    - Cybercrime Legalization in the African Region

- Why do we need Cyberlaws: The Indian Context
- The Indian IT Act
    - Admissibility of Electronic Records: Amendments made in Indian ITA 2000
    - Positive aspects of the ITA 2000
    - Weak Areas of the ITA 2000

- Challenges to Indian Law and Cybercrime Scenario in India
- Amendments to the Indian IT Act
  - Overview of changes made to the Indian IT Act
  - Impact of IT Act Amendments on Information Technology Organizations
- Cybercrime and Punishment
- Cyberlaw, Technology and Students: Indian Scenario

Understanding Computer Forensics

- Introduction
- Historical background of computer forensics
- The Need for Computer Forensics
- What is Computer Forensics?
  - What you can do with computer forensics
  - Incident Response vs. Computer Forensics
  - How computer forensics tools work
- Digital Forensics Life Cycle
  - The Digital Forensics Process
  - The Phases in Computer Forensics/Digital Forensics
  - Precautions to be taken while collecting Electronic Evidence
- Knowledge Base needed for Computer Forensics
  - Hardware
  - Operating Systems
  - Networks
- Learning Computer Forensics
  - Where and How to get training?
  - Where and How to get certified
- Gathering the Tools of the Trade
  - Write Blockers
  - Drive Kits
  - External Storage
  - Screwdriver Kits
  - Antistatic bags
  - Forensic Workstation
- Choosing Forensic Software
  - Open Source Software
  - Commercial Software
- Chain of Custody
  - Maintaining Chain of Custody
  - Evidence Tracking
- Storing Evidence
  - Securing your Evidence
  - Organizing your Evidence
  - Disposing of Old Evidence
- Challenges in Computer Forensics

  - Technical Challenges: Understanding the Raw Data and its Structure
  - The Legal Challenges in Computer Forensics and Data Privacy Issues

- Forensics Auditing
- Anti-forensics

Digital Forensics

- The Forensics data landscape
  - Active Data
  - Unallocated space
  - Slack space
  - Mobile Devices
  - External Storage

- Locations Where Evidence May Reside
  - Storage Media
  - Hardware Interfaces
  - File Systems
  - File Format
  - File Types
  - Header Analysis

- Recovering Data
  - Physical Damage
  - Logical Damage
  - File and Metadata Carving
  - Known File Filtering

- The Forensic Imaging
  - Forensic Imaging Method Pros and Cons

- Creating Forms
  - Chain of Custody Forms
  - Standard Operating Procedures Manual
  - Report Forms

- Live Forensics
  - When live forensics is the best option
  - Tools for Live forensics

- Capturing Evidence
  - Creating forensic images of Internal Hard drives
  - Creating Forensics Images of External Drives
  - Creating Forensics Images of Network Shares
  - Mobile Devices
  - Servers

- Non-traditional Digital Forensics
  - Non-traditional digital forensic techniques
  - Volatile Artifacts
  - Encrypted File Systems
  - Mobile Devices: Smart Phones and Tablets
  - Solid State Drives

- Virtual Machines

Forensics of Hand-Held Devices

- Introduction
- Understanding Cellular Device Concepts
  - The Basics
  - Understanding the types of Cellular Networks
  - Cell Phones: Hardware and Software Features
  - The Apps
- Hand-Held Devices and Digital Forensics
  - Mobile Phone Forensics
  - PDA Forensics
  - Smartphone Forensics
  - iPhone Forensics
  - Challenges in Forensics of the Digital Images and Still Camera
  - Forensics of the BlackBerry Wireless Device
- Toolkits for Hand-Held Device Forensics
  - EnCase
  - Device Seizure and PDA Seizure
  - Cellebrite
  - Magnet Acquire
  - Oxygen Software
- What evidence can you get from a Mobile Device
- Seizing Evidence from a Phone
- An illustration on Real Life Use of Forensics
- Techno-legal challenges with evidence from hand-held devices
  - Generally accepted evidence principles
  - Mobile phone evidence guidelines
  - Battery and memory storage considerations from forensics perspective

Forensic Analysis

- Hard Drive Specifications
  - General Harddrive Facts
  - RAID
- Characteristics of Physical Drives
  - Describe current hard drive technologies
  - Hard drive geometry
  - Calculate storage capacities using C.H.S and L.B.A
- Describe the boot process
  - The Boot Process and Drive Lettering
  - Identify the forensic issues associated with CMOS
  - Differentiate between operating systems and file systems
  - Limitations of using letters to define volumes
- What are we looking for?
  - Determining where the data went
  - LNK files
  - Shellbags

  - Recovering Log files
  - The Registry
  - Windows Swap file
  - Index.dat
  - Memory Analysis
  - How to deal with Encrypted drives and files

- Investigating Leaks
  - Reviewing the Registry Files
  - Identifying LNK files
  - Using File System Meta-data to investigate

- Email Forensics
  - How E-Mail works
  - Email Headers
  - Email files
  - Tracing Emails
  - Email Server Forensics

- The Recycle Bin
  - Function of the Windows Recycle Bin
  - Differences in the Recycle Bin on FAT and NTFS systems
  - What information can be recovered from the INFO2 file
  - What happens when a file is deleted or removed from the Recycle Bin
  - What happens when a user empties the Recycle Bin
  - How information can be retrieved when items are removed from Recycle Bin
  - Describe the forensic implications of files located in the Recycle Bin
  - Describe the function of the Orphan folder

- Common Windows Artifacts
  - Thumbs.db file
  - Define Thumbs.db behaviour
  - Identify thumbnail graphics

- Windows Registry
  - Function of the Windows registry
  - How the registry is organized
  - Forensic issues associated with multiple profiles on Windows systems
  - Registry Artifacts
    - NTUSER.DAT file
    - SAM file
    - SYSTEM file
    - SOFTWARE file
    - SECURITY file

- Tracking USB Devices
  - Function of the Mounted Devices Manager
  - Forensic benefits of tracking drive identification
  - Determine when removable media was last inserted in the system
  - Determine when removable media was first inserted in the system
  - Resolve who was logged on when a device was inserted
  - Other methods of identification of removable media

Network Forensics

- Network Packet Analysis
  - What is a Packet
  - Network Traffic Analysis
  - Log Files
  - HTTP Sniffer
  - Web Traffic
- Router Forensics
  - Router Basics
  - Types of Router Attacks
  - Gathering evidence from Router
- Firewall Forensics

Documentation and Reports

- Documenting your findings
  - What you were asked to do
  - What you reviewed
  - What you found
  - What your findings mean
- Types of Reports
  - Informal Report
  - Incident Report
  - Internal Report
- Explaining your work
  - Define Technical Terms
  - Explain Atifacts
  - Writing Reports for
  - Court Creating Exhibits

Electronic Discovery

- Electronic Discovery Reference Model - EDRM
- EDRM Life Cycle
- Phases in EDRM
  - Information Governance
  - Identification
  - Preservation
  - Collection
  - Processing
  - Review
  - Analysis
  - Production
  - Presentation
- Types of Investigation
- Liability and Proof
- Tools used for E-Discovery
- Relevant Laws