Digital Forensics Expert

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

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
  - o E-Mail Spoofing
  - o Cyber defamation
  - o Data Diddling
  - o Industrial Espionage
  - o Hacking
  - o Online Frauds
  - o Pornographic Offenses
  - o Software Piracy
  - o Computer Sabotage
  - o E-Mail Bombing
  - o Computer Network Instructions
  - o Password Sniffing
  - o Identity Theft
- Cybercrime: The Legal Perspectives
- Cybercrime: An Indian Perspective
- Cybercrime and Information Security
- Cybercrime and the Indian ITA 2000
  - o Hacking and the Indian Law(s)

CAREERS IN CYBERFORENSICS

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

CYBERCRIMES AND THE CYBERSECURITY: THE LEGAL PERSPECTIVES

- Introduction
- Cybercrime and the Legal Landscape around the World
  - o Online Safety and Cybercrime Laws
  - o Cybercrime Law Scenario in the Asia-Pacific Region
  - o Cybercrime and Federal Laws in the US
  - o The EU Legal Framework for Information Privacy to Prevent Cybercrime
  - o Cybercrime Legalization in the African Region
- Why do we need Cyberlaws: The Indian Context
- The Indian IT Act
  - o Admissibility of Electronic Records: Amendments made in Indian ITA 2000
  - o Positive aspects of the ITA 2000
  - o Weak Areas of the ITA 2000
- Challenges to Indian Law and Cybercrime Scenario in India
- Amendments to the Indian IT Act
  - o Overview of changes made to the Indian IT Act
  - o 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?
  - o What you can do with computer forensics
  - o Incident Response vs. Computer Forensics
  - o How computer forensics tools work
- Digital Forensics Life Cycle
  - o The Digital Forensics Process
  - o The Phases in Computer Forensics/Digital Forensics
  - o Precautions to be taken while collecting Electronic Evidence
- Knowledge Base needed for Computer Forensics
  - o Hardware
  - o Operating Systems
  - o Networks
- Learning Computer Forensics
  - o Where and How to get training?
  - o Where and How to get certified
- Gathering the Tools of the Trade
  - o Write Blockers
  - o Drive Kits
  - o External Storage
  - o Screwdriver Kits
  - o Antistatic bags
  - o Forensic Workstation
- Choosing Forensic Software
  - o Open Source Software
  - o Commercial Software
- Chain of Custody
  - o Maintaining Chain of Custody
  - o Evidence Tracking
- Storing Evidence
  - o Securing your Evidence
  - o 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

- o Windows Swap file
- o Index.dat
- o Memory Analysis
- o How to deal with Encrypted drives and files

- Investigating Leaks
  - o Reviewing the Registry Files
  - o Identifying LNK files
  - o Using File System Meta-data to investigate
- Email Forensics
  - o How E-Mail works
  - o Email Headers
  - o Email files
  - o Tracing Emails
  - o Email Server Forensics
- The Recycle Bin
  - o Function of the Windows Recycle Bin
  - o Differences in the Recycle Bin on FAT and NTFS systems
  - o What information can be recovered from the INFO2 file
  - o What happens when a file is deleted or removed from the Recycle Bin
  - o What happens when a user empties the Recycle Bin
  - o How information can be retrieved when items are removed from Recycle Bin
  - o Describe the forensic implications of files located in the Recycle Bin
  - o Describe the function of the Orphan folder
- Common Windows Artifacts
  - o Thumbs.db file
  - o Define Thumbs.db behaviour
  - o Identify thumbnail graphics
- Windows Registry
  - o Function of the Windows registry
  - o How the registry is organized
  - o Forensic issues associated with multiple profiles on Windows systems
  - o Registry Artifacts
- NTUSER.DAT file
- SAM file
- SYSTEM file
- SOFTWARE file
- SECURITY file
- Tracking USB Devices
  - o Function of the Mounted Devices Manager
  - o Forensic benefits of tracking drive identification
  - o Determine when removable media was last inserted in the system
  - o Determine when removable media was first inserted in the system
  - o Resolve who was logged on when a device was inserted
  - o Other methods of identification of removable media

Network Forensics

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

DOCUMENTATION AND REPORTS

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

Electronic Discovery

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