DIGITAL FORENSICS SYLLABUS

Module 1: Understanding Digital Forensics and Legal Aspects

- Understanding Computer Forensics
- Preparing for Computer Investigation
- Maintaining Professional Conduct
- Understanding Computer Investigations
- Taking a Systematic Approach
- Corporate Hi-Tech Investigations
- Conducting an Investigation

Module 2: Acquisition and Storage of Data

- Understanding Storage Formats for Digital Evidence
- Determining the Best Acquisition Method
- Contingency Planning for Image Acquisitions
- Using Acquisition Tools
- Validating Data Acquisitions
- Performing RAID Data Acquisitions
- Using Remote Network Acquisition Tools
- Storing Digital Evidence
- Obtaining a Digital Hash
- Sample Cases

Module 3: Working with Windows

- Understanding File Systems
- Exploring Microsoft File Structures
- Examining NTFS Disks
- Understanding Whole Disk Encryption
- Understanding the Windows Registry
- Understanding Microsoft Startup Tasks
- Understanding MS-DOS Startup Tasks

- Evaluating Computer Forensics Tool Needs
- Computer Forensics Software and Hardware Tools

Module 4: Working with Linux/Unix Systems

- UNIX and Linux Overview
- Inodes
- Boot Process
- Drives and Partition Schemes
- Examining Disk Structures
- Understanding Other Disk Structures
- Ownership and Permissions
- File Attributes
- Hidden Files
- User Accounts
- Case Studies
- Validating Forensic Data
- Addressing Data-Hiding Techniques
- Locating and Recovering Graphics Files

Module 5: Email and Social Media Forensics

- Investigating Email Crimes and Violations
- Applying Digital Forensics Methods to Social Media Communications
- Social Media Forensics on Mobile Devices
- Forensics Tools for Social Media Investigations

Module 6: Mobile Forensics

- Mobile Phone Basics
- Acquisition Procedures for Mobile Devices
- Android Device Forensics
- Android Malware
- SIM Forensic Analysis

- Case Study

Module 7: Cloud Forensics

- Working with Cloud Vendors
- Obtaining Evidence
- Reviewing Logs and APIs