

Digital Forensics – Advanced Computer Forensic Techniques (Mile2)

Course Number: ACFT

Length: 3 Day(s)

Certification Exam

This course will help you prepare for the following exams:

- **CCE:** Certified Computer Examiner
- **CFCE:** Certified Forensic Computer Examiner

Course Overview

This course follows up from the Digital Forensics & Electronic Discovery (CFED) course by providing insight into Laboratory Protocols, Processing Techniques, Crypto and Password Recovery, Specialized Artifact Recovery, and other areas.

Prerequisites

Students attending this course should have already completed:

- **CFED:** Digital Forensics & Electronic Discovery.

Audience

Advanced Computer Forensic Techniques is intended for law enforcement agents, legal professionals, corporate security personnel and other IT professionals who require systematic guidance on issues that arise in connection with electronic evidence in criminal and civil investigations.

Course Outline

- **Module 1 - Computer Forensic Investigative Theory**
- History of Digital Forensics
- Digital Evidence
- Three Main Aspects to Digital Evidence Reconstruction
- “Attack” Guidelines for the Recovery of Digital Data
- Classification
- Reconstruction
- Demo - TimeStomping
- Behavioral evidence analysis (BEA)
- Equivocal forensic analysis (EFA)
- Victimology

- Demo - Following the Clues from an Email Header
- Important Questions Regarding the Victim's Cybertrail
- Module 1 Review
- **Module 2 - Computer Forensic Laboratory Protocols**
- Overview
- QA
- SOP
- Notes
- Reports
- Peer Review
- Admin Review
- Annual Review
- Deviation
- Lab Intake
- Tracking
- Storage
- Discovery
- Module 2 Review
- **Module 3 - Computer Forensic Processing Techniques**
- Goal of Digital Evidence Processing
- Demo - Logical Review with FTK
- Duplication
- Documenting and Identifying
- Disassembling the Device
- Disconnecting the Device
- Document the Boot Sequence
- Removing and Attaching the Storage Device to Duplicated System
- Circumstances Preventing the Removal of Storage Devices
- Write Protection via Hardware/Software
- Geometry of a Storage Device
- Host Protected Area (HPA)
- Tools for Duplicating Evidence to Examiner's Storage Device
- EnCase for Windows Acquisition Tool
- Demo - Hashing and Duplicating a Drive
- Preparing Duplication for Evidence Examination
- Recording the Logical Drive Structure
- Using “Sandra” and “WinHex”
- File Allocation Tables
- Logical Processes
- Known Files
- Reference Lists
- Verify that File Headers Match Extensions
- Demo - Introduction to FTK
- “Regular Expressions”
- Demo - Using Regular Expressions
- File Signatures

- Demo - Hex Workshop Analysis of Graphic Files
- Module 3 Review
- **Module 4 - Crypto and Password Recovery**
- Background
- Demo - Stegonography
- History
- Concepts 1
- Demo - Cracking a Windows Hashed Password
- Concepts 2
- File Protection
- Options 1
- Demo - Recovering Passwords from a Zip File
- Options 2
- Rainbow Tables
- Demo - Brute Force/Dictionary Cracks with Lophtrcrack
- Demo - Password Cracking with Rainbow Tables
- Module 4 Review
- **Module 5 - Specialized Artifact Recovery**
- Overview
- Exam Preparation Stage
- Windows File Date/Time Stamps
- File Signatures
- Image File Databases
- Demo - Thumbs.DB
- The Windows OS
- Windows Operating Environment
- Windows Registry
- Windows Registry Hives 1
- Demo - Registry Overview
- Windows Registry Hives 2
- Windows 98 Registry
- Windows NT/2000/XP Registry
- Windows Registry ID Numbers
- Windows Alternate Data Streams
- Demo - Alternate Data Streams
- Windows Unique ID Numbers
- Other ID's
- Historical Files 1
- Demo - Real Index.dat
- Historical Files 2
- Demo - Review of Event Viewer
- Historical Files 3
- Demo - Historical Entries in the Registry
- Historical Files 4
- Windows Recycle Bin
- Demo - INFO Files

- Outlook E-Mail
- Outlook 2k/Workgroup E-Mail
- Outlook Express 4/5/6
- Web E-Mail
- Module 5 Review