

FORENSIC TRACK

FT440, Advanced Forensic Concepts (AFC)

Who Should Attend

DoD and federal law enforcement agents who will be called upon to perform forensic analysis of digital media.

Prerequisites

TT110 (INCH), RT120 (CIRC) and FT210 (WFE-E) or FT215 (WFE-FTK) or Test outs

Duration

5 Days

Course Description

Examines advanced digital forensic concepts not typically addressed at the basic or intermediate level. Lessons will broaden the capabilities of examiners, agents and analysts, by presenting tools and methods for: examining NTFS Master File Table records and windows hibernation file; advanced windows registry analysis; recovering deleted partitions and rebuilding raids; Imaging and analyzing volatile data; identifying artifacts; overcoming passwords and encryption; and detecting and analyzing steganographic files.

Objectives

- Identify advanced data recovery scenarios and choose appropriate advanced examination solutions to recover digital artifacts
- Identify and attack common encryption techniques using a variety of methods and explain their significance to forensic examinations
- Use advanced techniques to overcome password protected systems and files
- Use advanced techniques to capture and analyze Volatile Memory
- Use advanced forensic recovery techniques to identify and recover information of investigative relevance from digital media

Topics Covered

Introduction to Advanced Forensic Concepts

- Introduction to Advanced Forensic Concepts

Virtual Machines

- Introduction to Virtual Machines and VMware
- Live View

Advanced Windows Forensic Analysis

- Advanced Analysis of Windows System Files and Windows Registry

Partition Recovery

- Partition Recovery

RAID Imaging and Recovery

- Hardware and Software RAIDs
- Rebuilding RAIDs with EnCase

Encryption and Steganography

- Introduction to Encryption and Encrypted Volumes
- Advanced Password Cracking with Cain and Abel
- Steganography

FORENSIC TRACK

Web Usage Analysis

- NetAnalysis and HstEx
- File Sharing Environments
- Social Networking

Preparation

To assist in your preparation for AFC, we recommend the following:

You should be familiar with:

- Virtual Machine Technologies
- The Windows Registry
- Hard Drive Partitioning
- Current Encryption Technologies
- Volatile Data
- NetAnalysis and History Extractor (HstEx)
- Internet Artifacts

You should review the following topics:

- WFE-EnCase:
 - Windows Registry Lesson
 - Partition Information Lesson
 - Web Related Evidence Lesson
 - Instant Messaging Lesson
- VMware (VMware, Inc.)
- VirtualBox (Oracle, Inc.)
- LiveView (Carnegie Mellon University)
- TrueCrypt
- Analysis of Hardware and Software RAID Configurations
- Microsoft's Encrypting File System (EFS)
- Physical Memory (RAM)
- Memory Limits for Windows Releases
- Guidelines for Evidence Collection and Archiving
- DigitalDetective

You should know:

- The Order of Volatility as Expressed in RFC3227

These topics are covered in DCITA courses you may have attended previously and can also be found on the dcita.edu portal (<https://www.dcita.edu>), the internet, at Books 24/7, in your organization's technical library or at the public library.

AFC Grading Policy

The minimum passing score on all Knowledge and Performance Tests is 70%. Students who fail any Knowledge or Performance Test other than the final exam are given remedial training and tested again. If a student fails a re-test, the student fails the course. If a student fails the final Knowledge or Performance Exam, a re-test will not be given and the student fails the course.

In the Advanced Forensic Concepts course, the student's progress is monitored through instructor observation during lecture, discussion and practical exercises as well as Knowledge and comprehensive Performance Tests.