Advanced FTK

Advanced • Three-Day Instructor-Led Course

For more information contact: info@syntricate.com

The AccessData® Advanced FTK class provides the knowledge and skills necessary to effectively use the advanced analysis features of FTK™, FTK Imager™ Password Recovery Toolkit™ (PRTK™) and Registry Viewer™.

During this three-day, hands-on course, participants will perform the following tasks:

- Use FTK's advanced processing options to examine evidence
- Merging index, setting preferences, saving cases
- Managing shared objects both at a global level and a case level
- Gain and understanding of processing options and profiles
- Use filtering to locate items of interest quickly
- Examine Live and Index searching, including TR1 Regular Expressions
- Utilize Cerberus to locate possible malware
- Use Visualization to get a graphic timeline view of files and Internet history.
- Use Geolocation to identify where photos were taken
- Remote data preview and acquisition features
- Understand the requirements and how to setup Distributed Processing
- Obtain live memory and volatile data from a target system and complete an analysis of the data

Prerequisites:

This hands-on course is intended for users who have previously attended the AccessData BootCamp training, particularly forensic professionals and law enforcement personnel, who use AccessData forensic software to examine, analyze, and classify digital evidence.

- Previous AccessData BootCamp training
- Able to understand course curriculum presented in English
- Perform basic operations on a personal computer
- Have a basic knowledge of computer forensic investigations

(Continued on other side)

SYNTRICATE

Advanced FTK

Advanced • Three-Day Instructor-Led Course

For more information contact: info@syntricate.com

(Continued)

Module 1: Introduction

Topics:

- Identify the LAB components
- List the LAB and PRTK system requirements
- Describe how to receive upgrades and support for AccessData tools

Module 2: Case Setup

Objectives:

- Merging Index
- Optimum Setup for FTK
- Preferences
- Archive/Backup
- Restore
- Indexing Options

Module 3: Advanced Processing (Part 1)

Objectives:

- Managing Shared Objects
  - Carvers
  - Custom Identifiers
  - Columns
  - File Extension Maps
  - Filters
  - Labels
- Photo DNA
- Evidence Processing Profiles

Module 4: Advanced Processing (Part 2)

Objectives:

- Managing Shared Objects
- Photo DNA
- Windows Event Logs
- Prefetch files
- Explicit Image Detection
- Optical Character Recognition
- Examining Video Files

Module 5: Advanced Filtering

Objectives:

- Designing Filters
- Compound Filters
- Global Filters
- Tab Filters

Module 6: Advanced Searching Techniques

Objectives:

- Live Search Options
  - Text
  - Pattern
  - Hex
- Index Search
  - dtSearch Indexing Options
  - Conducting an Index Search
  - Importing/Exporting Search Terms
  - Search Operators
  - Searching for a phrase
  - Boolean Searches
  - Searching Options
  - TR1 Regular Expressions

Module 7: Cerberus

Working with Registry Viewer

Objectives:

- What is Cerberus Analysis
- Cerberus Processing Stages
- Stage 1 Analysis
- Stage 1 Threat Scoring
- Stage 2 Analysis
- Stage 2 Report
- Running Cerberus Analysis
- Reviewing Results in Examiner
- Exporting a Cerberus Report
- Bookmarking & Reporting Cerberus Files

SYNTRICATE

Advanced FTK

Advanced • Three-Day Instructor-Led Course

For more information contact: info@syntricate.com

(Continued)

Module 8: Visualization

Objectives:

- Launching Visualization
- Visualization Page
- Themes
- Visualization of Data
  - Files
  - Emails
  - Social Analysis
  - Traffic
  - Internet Browser History
- Geolocation

Module 9: Adding Remote Evidence

Objectives:

- Describe the Remote Disk Mounting Service (RDMS)
- Deploy Temporary Agents
- Access Remote Data with Temporary Agent
- Create Digital Certificates
- Deploy Enterprise Agents
- Access Remote Data with Enterprise Agent
  - Including Memory
- Mount a drive remotely
- Preview and Image a drive remotely

Module 10: Distributed Processing

Objectives:

- Describe the benefits of Distributed Processing
- System Requirements
- Installing DPE software

Module 11: Volume Shadow Copy

Objectives:

- Describe how Volume Shadow Copy works
- Identify what forensic information can be recovered from Volume Shadow Copy
- Use FTK to process a restore point

Module 12: Memory and Volatile Data Analysis

Objectives:

- What is memory vs. volatile data
- Capturing RAM
- Obtaining volatile data
- Adding to case
- Volatile tab
- Reporting

SYNTRICATE