

Forensic Fundamentals

Beginner • Three-day Instructor-led Class



AccessData®

The AccessData® Forensic Fundamentals course provides an introduction to computer forensics.

During this three-day, hands-on course, participants will review the following concepts:

- Sources of electronic evidence
- Current challenges facing forensic examiners
- Search and seizure issues
- How data is stored including a review of:
 - Bit
 - Nibble
 - Byte
 - Word
 - Binary
 - Decimal
 - Hexadecimal
 - ASCII and Unicode character sets
- Hard drive geometry and physical characteristics of storage media
- Drive partition schemes (Primary vs. Extended partitions)
- Logical drives and physical drives
- The boot process and how drive letters are assigned
- File system vs. operating system functions
- FAT12, FAT16, and FAT32 file systems
- File Allocation Tables
- Deleted file recovery
- Accessing drives with Write Blocking Technology
- Imaging drives with FTK Imager
- Validating image file integrity
- Basic evidence analysis with FTK

Course Materials and Software

You will receive the student training manual and CD containing the training material, lab exercises and course-related information.

Module 1: Introduction

Topics

- Introductions
- Course materials and software
- Prerequisites
- Course outline
- Helpful Information

Lab

- Check system information.
- Select Windows Explorer display preferences.
- Prepare your system.

Module 2: What is Computer Crime?

Objectives

- Describe how computer technology is used in high tech crime.
- Review current challenges facing the forensic examiner.
- Discuss evidence gathering techniques.

Module 3: Search and Seizure Issues

Objectives

- Review pre-search considerations.
- Identify sources of electronic evidence.
- Describe how to take control of a computer during a seizure.
- List shutdown issues.

Module 4: Introduction to FTK Imager

Objectives

- List standard data storage devices.
- List which file systems FTK Imager can read.
- Review the FTK Imager interface.
- Describe the information provided in the FTK Imager Properties and Interpreters windows.
- Preview local physical devices in FTK Imager.

Lab

- Install FTK Imager.
- Review the FTK Interface.
- Preview the local hard drive.

Module 5: Numbering Systems

Objectives

- Describe how computers view data.
- Define bit, nibble, byte and word.
- Identify binary, decimal, and hexadecimal data.
- Differentiate between ASCII and Unicode characters.

Module 6: Characteristics of Physical Drives

Objectives

- Identify and list the physical characteristics of floppy disk and removable media.
- Describe current hard drive technologies.
- Describe hard drive geometry:
 - Sectors
 - Tracks
 - Heads
 - Cylinders
- Calculate storage capacities using C.H.S. and L.B.A.

Module 7: Partitioning Concepts

Objectives

- Differentiate between logical drives and physical drives.
- Describe how drive partitions are used.
- Describe the master partition table:
 - Identify the location of the partition table.
 - Identify the size of the table.
 - Identify the size of each entry.
 - Identify partition type codes.
- List common partition types

Lab

- Create primary and extended partitions and logical drives.
- Preview the partitions in FTK Imager.

Module 8: The Boot Process and Drive Lettering

Objectives

- Describe the boot process.
- Identify the forensic issues associated with CMOS.
- Differentiate between operating systems and file systems.
- Identify the limitations of using letters to define volumes.
- List rules DOS uses to assign drive letters.

Module 9: Formatting FAT

Objectives

- List the FAT file system components.
- List the three components that make up the system area on a drive formatted to FAT.
- Identify system area differences between FAT16 and FAT32.
- Describe what data clusters are.
- Describe how the *format* command affects existing data.

Lab

- Format logical partitions to FAT 16 and FAT 32.
- View the system areas with FTK Imager.
- Copy data to the new partitions, then format the partitions and observe the effects on the data.

Module 11: The File Allocation Table

Objectives

- Describe the function of the File Allocation Table.
- List the limitations of addressing clusters with FAT12, FAT16 and FAT32.
- Describe the four possible FAT entry values.

Lab

- Use FTK Imager to view the System area.
- Use FTK Imager to view how files are managed in the File Allocation Table.

Module 12: Saving Files and Directories in FAT

Objectives

- Describe the changes that occur when a file, folder, or subfolder is created and saved.
- Identify the key elements of a directory entry.
- Describe the rules for short and long file names.
- Describe the concept of file slack.
- Create files and folders on a FAT16 and FAT32 drive.

Lab

- Observe the effects of creating and saving files with short and long filenames in a FAT16 partition.
- Observe the effects of creating and saving folders and subfolders in a FAT16 partition.

Module 13: Deleted File Recovery in FAT

Objectives

- Describe what happens when files and folders are deleted on a FAT system.
- List the effects of data when files are deleted.
- Describe how to manually recover a deleted file.
- Describe how to recover deleted file fragments.

Lab

- Observe what happens when a file or Folder is deleted on a FAT volume.
- Manually recover deleted files on a FAT volume.

Module 14: Drive Access and Write Blockers

Objectives

- Identify the issues associated with Int 13, Int 13x, Direct access, and Windows access.
- Identify the limitations of software write blockers.
- Describe the host protected area.
- Identify write blocking devices.

Lab

Create a registry key and import it to the local machine registry to prevent the operating system from making changes to the registry when using USB storage devices.

Module 15: Imaging

Objectives

- Compare the following imaging processes:
 - File by file copy
 - Bit stream image
- Describe file system considerations when acquiring logical volumes.
- List the image formats FTK Imager supports.
- Use hash algorithms to validate image file integrity.

Module 16: Introduction to FTK

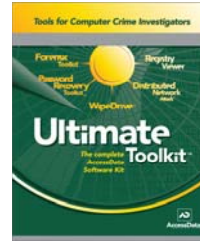
Objectives

- Review the main FTK interface.
- Describe the function of the menu commands, toolbars, and tabs.
- Start a case in FTK.
- Describe the following FTK analysis processes:
 - File identification
 - Data carving
- Preview an image in FTK.

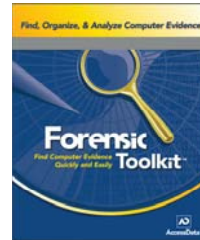
Practical Skills Assessment

The Forensic Fundamentals course includes an optional Practical Skills Assessment (PSA). This performance-based assessment requires participants to apply key concepts presented during the course to complete a practical exercise. Participants who successfully complete the exercise receive a PSA certificate of completion.

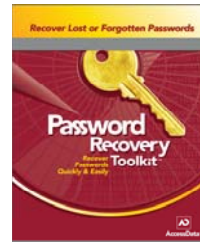
For a complete listing of scheduled courses or to register for available courses, see www.dataduplication.co.uk.



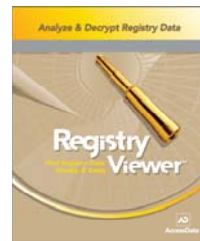
Ultimate
The Complete
AccessData
Software Kit
Toolkit™



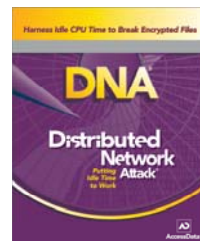
Forensic
Find Computer Evidence
Quickly & Easily
Toolkit™



Password
Recover
Passwords
Quickly & Easily
Recovery
Toolkit™



Registry
Find Registry Data
Quickly & Easily
Viewer™



Distributed
Putting
Idle Time
To Work
Network
Attack™

© 2006 AccessData Corporation – All rights reserved.

Some topics and items in this course syllabus are subject to change. This document is for information purposes only. AccessData makes no warranties, express or implied, in this document. AccessData, Forensic Toolkit, FTK, FTK Imager, Known File Filter, KFF, Password Recovery Toolkit, PRTK, Registry Viewer, and Ultimate Toolkit are either registered trademarks or trademarks of AccessData Corporation in the United States and/or other countries. Other trademarks referenced are property of their respective owners.