



A Knowledge and Practical Based
Preparation for the
AccessData Certified Examiner
Credential

AccessData
Training



Unless otherwise noted, the companies, organizations, products, e-mail addresses, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, e-mail address, person, places or events is intended or should be inferred. Complying with all copyright laws is the responsibility of the user.

No part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of AccessData Corporation.

AccessData may have trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from AccessData, the furnishing of this document does not give you any license to these trademarks, copyrights, or other intellectual property.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright ©1987–2008 AccessData Corporation.

All rights reserved.

AccessData Certified Examiner Study Guide
August 7, 2008

AccessData Corporation
384 South 400 West
Lindon, UT 84042
U.S.A.
www.accessdata.com

AccessData Trademarks

AccessData is a registered trademark of AccessData Corp.

AccessData Certified Examiner is a registered trademark of AccessData Corp.

ACE is a registered trademark of AccessData Corp.

Distributed Network Attack is a registered trademark of AccessData Corp.

DNA is a registered trademark of AccessData Corp.

Forensic Toolkit is a registered trademark of AccessData Corp.

FTK is a registered trademark of AccessData Corp.

FTK Imager is a trademark of AccessData Corp.

Password Recovery Toolkit is a registered trademark of AccessData Corp.

PRTK is a registered trademark of AccessData Corp.

Registry Viewer is a registered trademark of AccessData Corp.

Ultimate Toolkit is a registered trademark of AccessData Corp.

UTK is a registered trademark of AccessData Corp.

Third Party Trademarks

All third-party trademarks belong to their respective owners.

CONTENTS

AccessData Certified Examiner Program Overview

Prerequisites	1
Test-Out Process	2
Certification Process	2
Section 1	2
Section 2	2
ACE Preparation	3

Study Guide

FTK Imager	5
FTK Imager Lab	8
Forensic Toolkit 2	9
FTK2 Lab	15
User Accounts	15
Case Creation	15
Tabs	15
Bookmarking	15
Column Settings	16
Report Wizard Options	16
Data Carving	16
File Filtering	16
Processing	16
Known File Filter (KFF)	16
Registry Viewer	17
Registry Viewer Lab	18
Password Recovery Toolkit	19
Password Recovery Toolkit Lab	21
Utility Integration	22

Knowledge-Based Assessment Sample Questions 23
Arrest Booking Sheet 27
A Police Department Near You 27

SECTION 1

AccessData Certified Examiner Program Overview

The AccessData Certified Examiner (ACE) program certifies proficiency for the following AccessData products: Forensic Toolkit 2 (FTK), FTK Imager, Password Recovery Toolkit (PRTK) and Registry Viewer.

The ACE credential provides corporate and law enforcement agencies a competency metric for knowledge and practical application of the AccessData tools.

PREREQUISITES

Candidates pursuing the ACE credential must meet the following pre-requisites:

- Possess licensed copies of the Forensic Toolkit 2 (FTK), Password Recovery Toolkit (PRTK) and Registry Viewer. (FTK Imager is free). Software subscription must be current when candidate begins the process.
- Complete the following AccessData certified training courses:
 - AccessData BootCamp (FTK2)
 - Windows Forensics (FTK2)
- Have six months of forensic examination experience. A letter (written and signed by your supervisor) documenting the prerequisite six months of examination experience will be required. The letter should be submitted on agency/organization letterhead. Your supervisor's contact information is also required so your experience can be validated.

Note: During the initial transition period to FTK2 technology there may be varying class requirements depending on the background of the ACE candidate. Please contact a sales representative or email ace@accessdata.com for further information.

TEST-OUT PROCESS

Those candidates wishing to be exempted from the class attendance requirement may opt for the ACE Test-Out.

- Candidates may attend an ACE Test-Out session to demonstrate their abilities with the software by participating in a proctored, timed practical based skill assessment.
- Candidates have 60 minutes to complete the skill assessment.
- If the candidate fails a Test-Out session, they must complete the ACE Prep course to attempt the Test-Out session again.
- If the candidate fails a second Test-Out session, they must complete the class pre-requisites to challenge the ACE process.

CERTIFICATION PROCESS

The certification process is a one-day proctored procedure. Candidates must successfully complete both sections of the examination to obtain the ACE certification:

Section 1

Candidates must successfully complete the knowledge-based assessment (KBA) with an 80% or higher score.

The KBA is administered by Thomson Prometric.

Section 2

Candidates must successfully complete a practical-based assessment (PBA) that will consist of multiple exercises.

ACE PREPARATION

The AccessData Certified Examiner credential is obtained by completing the KBA (Knowledge Based Assessment) and the PBA (Practical Based Assessment) administered through AccessData.

Prerequisites for ACE include the AccessData BootCamp and Windows Forensics courses or the ACE Test-Out. The certification is tool-centric. The process does not include a legal section.

In preparation for the ACE program, it is recommended that students utilize their training manuals from the prerequisite courses as study guides. Focusing on the learning points and lab exercises from the course modules will best prepare the ACE candidate for test questions and practical assessment activities in the ACE process.

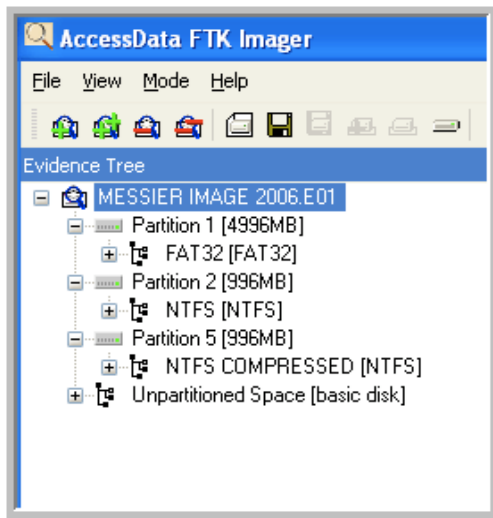
For more information, send email to ace@accessdata.com or see <http://www.accessdata.com/training>.

SECTION 2

Study Guide

FTK IMAGER

- 1 When previewing a physical drive with FTK Imager, you observe 3 logical volumes numbered 1, 2 and 5. Explain the drive numbering system.



2 True or False FTK Imager includes write blocking software.

3 Name five file systems that can be read by FTK imager.

3a _____

3b _____

3c _____

3d _____

3e _____

4 List the four types of evidence you can add to FTK Imager.

4a _____

4b _____

4c _____

4d _____

5 Name five image formats that can be read by FTK Imager.

5a _____

5b _____

5c _____

5d _____

5e _____

6 If you convert a Raw (dd) image to an E01 image, will the image hash values match? Explain.

7 Name the three image files that can use compression.

7a _____

7b _____

7c _____

FTK Imager Lab

AccessData software users can create images using FTK Imager. FTK Imager creates four image format types: DD, Smart*, Encase*, and FTK Custom Content Image. Using Isobuster* technology, FTK Imager can also create CD and DVD image files (created as ISO and CUE files). In addition to creating images, FTK Imager can be used to acquire live files locked by the Windows* environment.

Imaging-Thumb drive _____

- multiple images _____
- image summary file info _____

Export Image _____

- verify process _____

Load image file _____

- partition numbering _____
- file systems _____
- properties _____
- Hex Interpreter _____

Export files _____

- recursive export _____

Create hash list _____

- file extension _____
- file info _____

Acquire registry files _____

Custom Content Image _____

FORENSIC TOOLKIT 2

1 What are the two types of user accounts in FTK2?

1a _____

1b _____

2 Case Reviewers can review cases but do not have the rights to:

2a _____

2b _____

2c _____

2d _____

2e _____

2f _____

2g _____

3 Name the two ways FTK2 and the KFF identify files.

3a _____

3b _____

4 All case items are listed in only one of the File Category containers. How does FTK2 determine file category?

- 5 In which container would you find the following file types:
- Zip files _____
 - AVI or MPEG files _____
 - Registry Files _____

6 A .jpg graphic is attached to an email message. In which FTK2 tabs and containers would you find this file?

7 In the **Explore** tab, how do you view all case files or selected directories and sub-directories?

8 Name three target items in FTK2.

8a _____

8b _____

8c _____

9 What are the benefits of using the FTK Full Text Index?

10 List six types of evidence that can be added to FTK2.

10a _____

10b _____

10c _____

10d _____

10e _____

10f _____

11 List three additional Analysis Tools.

11a _____

11b _____

11c _____

12 What are the four types of views in the File Content pane?

12a _____

12b _____

12c _____

12d _____

13 In the **Overview** tab, the Case Overview is broken down into five primary containers. What are they?

13a _____

13b _____

13c _____

13d _____

13e _____

14 How can an examiner create or remove custom tabs?

15 In the **Bookmark** tab, the examiner can add, remove, or modify what information for bookmarked files?

15a _____

15b _____

15c _____

15d _____

15e _____

15f _____

16 Define Copy Special and File Export.

17 What is the purpose of marking files as privileged?

18 List the windows that make up the FTK2 Report Wizard.

18a _____

18b _____

18c _____

18d _____

18e _____

18f _____

19 What is the difference between the Data Carve and Meta Carve functions?

20 In what two forms can an email message be exported?

20a _____

20b _____

FTK2 LAB

User Accounts

- Admin/DB Admin _____
- Reviewer _____

Case Creation

- processing options _____
- add evidence _____

Tabs

Overview

- Containers _____
- Numbers _____

Explore

- QuickPick _____
- Graphics _____
- Live Search _____
- Indexed Search _____
- Bookmark _____

Bookmarking

- Parents _____
- Comments _____
- Selections _____
- Attachments _____

Column Settings

- Object Name, File Type, Cr Date, Mod Date, Acc Date
- Export & Import option _____

Report Wizard Options

- Case Information _____
- Bookmarks _____
- Graphics _____
- File Paths _____
- File Properties _____
- Case Log _____
- Registry Selections _____

Data Carving

- File Types _____
- Limit by size _____

File Filtering

- Global vs. Nesting _____
- Import & Export _____

Processing

- Metadata _____
- Link Files _____
- Recycle Bin _____

Known File Filter (KFF)

- Groups _____
- Importing _____

REGISTRY VIEWER

1 Name and describe six Registry Viewer functions.

1a _____

1b _____

1c _____

1d _____

1e _____

1f _____

1g _____

1h _____

2 List three ways to use the Summary Reports function.

2a _____

2b _____

2c _____

REGISTRY VIEWER LAB

Common Areas _____

Searching _____

Hex Interpreter _____

Regular Report _____

Summary Report _____

PSSP _____

SAM _____

PASSWORD RECOVERY TOOLKIT

1 In PRTK, which type of attack uses word lists?

2 List and define three additional PRTK attacks.

2a

2b

2c

3 List and define the first level of attack.

4 What kind of information can PRTK recover from the USER.DAT or NTUSER.DAT files?

5 Where can a user determine what type of attack will be performed on a file?

6 What is the most effective method to facilitate successful password recovery?

7 What three parts comprise an Attack Profile?

7a _____

7b _____

7c _____

8 What happens to a file's hash value once it is decrypted?

Password Recovery Toolkit Lab

Attack Profiles

- Import wordlist from FTK2 _____
- Biographical Dictionary (see *Arrest Booking Sheet* on page 27)
- Create Attack Profile _____

AccessData Decryption Methodology

- Export encrypted files _____
- Decrypt files _____
- Import decrypted files to FTK2 _____
- Repeat wordlist export and decryption _____

Windows logon passwords

- SAM and System files _____

Utility Integration

1 What applications can be launched within FTK2?

1a _____

1b _____

1c _____

1d _____

2 Which registry files can be selected from the FTK2 Report Wizard to be included in a report?

2a _____

2b _____

2c _____

Other Integrated Functions

- Export Wordlist (with registry files) from FTK2
- Create hash set in Imager; import into FTK2
- Use Imager to obtain registry files and analyze in Registry Viewer
- EFS decryption using FTK2 and PRTK
- Export registry wordlist from Registry Viewer to PRTK
- Decrypt Office documents and EFS files in FTK2

KNOWLEDGE-BASED ASSESSMENT SAMPLE QUESTIONS

- 1** In FTK2, how would a user view all of the graphics in the case in the Sorts the graphic with a custom filter.
 - a** Select the root of the evidence in the Evidence Items pane.
 - b** Use the QuickPicks option in a directory.
 - c** Use the QuickPicks option at the top of the evidence listing in the Graphics tab.
 - d** Select the Explore tab and use the QuickPicks at the top of the evidence listing.

- 2** Which two FTK2 feature allow you to export properties about an item rather than the item itself?
 - a** Export File
 - b** Copy Special
 - c** Export File List Info
 - d** Column Settings

- 3** Which three are valid sections of an FTK2 report?
(Choose three)
 - a** File Paths
 - b** Registry Selections
 - c** List by File Header
 - d** Bookmarks
 - e** List Evidence Items by Path

- 4 What are the two Hash values in the KFF?
(Choose two)
- a Alert
 - b Hide
 - c Show
 - d Ignore
 - e Important
- 5 If you add additional Hash values to the case after it has been processed, what must you do to utilize the new KFF values in the current case?
- a Select **Evidence > Additional Analysis > KFF Lookup > Do not check previously processed items.**
 - b Select **Tools > Preferences > KFF Lookup > Do not check previously processed items.**
 - c Select **Evidence > Additional Analysis > KFF Lookup > Recheck previously processed items.**
 - d Select **Tools > Preferences > KFF Lookup > Recheck previously processed items.**
- 6 Which of the following statements about the PRTK Biographical Dictionary are true?
- a It helps to create an overall picture of the computer user.
 - b Data can be input in any category without affecting effectiveness.
 - c The resulting dictionary creates permutations of input terms.
 - d The Biographical Dictionary contains locally recovered passwords.

- 7 What information can PRTK recover from the NTUSER.DAT file? (Choose two)
- a Web passwords
 - b Windows logon passwords
 - c Instant Messenger passwords for Yahoo! or AIM
 - d List of all EFS files on suspect images
- 8 Which two statements are true about the Full Text Index in FTK2? (Choose two)
- a Can be used as a dictionary in PRTK
 - b It is necessary for Data Carving in FTK2
 - c It is essential for Analysis Tools in FTK2
 - d It is required for Index Searching in FTK2
 - e It is required for Live Searching in FTK2
- 9 How can you use an FTK Imager File Hash List?
- a It can be used to document a file's encrypted status
 - b It can be integrated into FTK2 Data Carving
 - c It can be imported into an existing KFF database
 - d It can be used as a PRTK word list
- 10 In Registry Viewer, how would you create a report that can be utilized in future cases?
- a Select **Edit > Create Global Report**
 - b Select **Report > Define Summary Report**
 - c Select **Report > Manage Summary Report**
 - d Select **Edit > Define Summary Report**

- 11** In Registry Viewer, how would you select only items in the registry that may contain important information?
- a** Select Edit > Find Summary Data
 - b** Select Report > Manage Common Report
 - c** Select View > Common Areas
 - d** Select View > Display Summary Data
- 12** In FTK Imager, which file formats allow for compression? (Choose three.)
- a** dd images
 - b** .e01 images
 - c** .tar images
 - d** .s01 images
 - e** .ad1 images
- 13** In FTK2, what file image formats use the command to Verify Image Integrity? (Choose two.)
- a** dd images
 - b** .e01
 - c** .s01
 - d** .ad1 images

ARREST BOOKING SHEET

A Police Department Near You

Name: John William Smith

Alias: Big John
John John
Johnny
Willis Smith
JW

Street: 1384 Peachtree Drive

City: Draper

State: UT

Zip Code: 84020

Country: USA

Phone: 900-225-7788

SSN: 202-34-1234

DOB: 10/31/1975

Tattoos: Left Forearm - Wording "Geterdone"

Contact: Sally Porter (Mother) 900-555-4515

Narrative: At the time of arrest, SMITH was traveling with two children:

TONYA SMITH (DOB 11/08/1999)
PHIL SMITH (DOB 05/14/1997)

SMITH was traveling in a 1967 red Corvette Stingray with the license plate "VETTS ROCK."

