

Password Recovery Toolkit 100

Advanced Two-Day Instructor - Led Course

For more information contact: training@accessdata.com

The AccessData Password Recovery Toolkit 100 – Two-Day course you will learn how to locate different types of encrypted files and the different ways to attack the encryption. You will learn ways to make a custom dictionary that will help improve your ability of breaking the encryption. You will also learn how to setup and use DNA which will increase your chances of breaking into the encrypted file.

Prerequisites

This two-day hands-on class is intended for new and advanced users. This class particularly caters to forensic professionals and law enforcement personnel, who use AccessData forensic software to examine, analyze, classify and decrypt digital evidence.

To obtain the maximum benefit from this class, you should meet the following requirements:

- Able to understand course curriculum presented in English
- Perform most operations on a personal computer
- Have a moderate knowledge of computer forensic investigations and acquisition procedures
- Be very familiar with the Microsoft Windows environment
- Have moderate experience with FTK and its component software

Class Materials and Software

You will receive the associated materials prior to the course.

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

- Be able to identify and locate encrypted files
- Determine the best method for decrypting encrypted files
- Be able to create custom profiles to attack the encrypted files
- Know how to setup and use PRTK / DNA in your office

The course includes multiple hands-on labs that allow students to apply what they have learned in the workshop.



Some topics and items in this class syllabus are subject to change. This document is for information purposes only. AccessData makes no warranties, express or implied, in this document. AccessData, AccessData Certified Examiner, ACE, Distributed Network Attack, DNA, Forensic Toolkit, FTK, LAB, Password Recovery Toolkit, PRTK, Registry Viewer, and Ultimate Toolkit are registered trademarks of the AccessData Group, LLC. in the United States and/or other countries. Other trademarks referenced are property of their respective owners.

Password Recovery Toolkit 100

Advanced Two-Day Instructor - Led Course

For more information contact: training@accessdata.com

Module 1: Introduction

Topics:

- Cryptography terminology
- Discuss the types of encryption
- Discuss the types of passwords
- The concept behind XOR
- Symmetric encryption
- Asymmetric encryption

Module 2: Accessdata Software

Objectives:

- Install AccessData FTK Imager
- Install AccessData PRTK / DNA
- Install AccessData Registry Viewer
- Discuss processing options

Lab:

Participants will process a forensic image and identify the encrypted files to be decrypted and decrypt them

Module 3: FTK Toolkit

Topics:

- Custom processing profiles
- Custom columns
- Exporting a word list
- Accessdata art of War

Lab:

During this practical, students will identify the encrypted files and export the correct files to be decrypted. They will then create a custom profile used to obtain the needed password

Module 4: PRTK / DNA

- Rules, Profiles and Preferences
- Explain creating custom profiles
- Choosing the right rules
- Creating custom rules
- Discuss attack types

Module 5: Dictionaries

Objectives:

- How to make dictionaries
- Biographical dictionaries
- Passphrase dictionaries
- Permutation dictionaries
- Strings command
- WebCrawler's like HTTrack

Lab:

Students will use different dictionaries they have learned how to build to find the password to the encrypted files in this case.

Module 6: Encrypted Containers

Objectives:

- Be able to locate encrypted Containers
- BitLocker
- TrueCrypt
- VeraCrypt
- Invisible Secrets

Lab:

Students will learn to use Imager and Header extract to carve off the header of the file and bring it into PRTK for decryption.

Module 7: Student Practical

Objectives:

- Students will apply all knowledge learned from this course on the scenario.
- Students will locate the encrypted files:
- Export a word list
- Create a custom profile
- Decrypt the files inside FTK
- Export files and Decrypt them using PRTK



Some topics and items in this class syllabus are subject to change. This document is for information purposes only. AccessData makes no warranties, express or implied, in this document. AccessData, AccessData Certified Examiner, ACE, Distributed Network Attack, DNA, Forensic Toolkit, FTK, LAB, Password Recovery Toolkit, PRTK, Registry Viewer, and Ultimate Toolkit are registered trademarks of the AccessData Group, LLC. in the United States and/or other countries. Other trademarks referenced are property of their respective owners.