Password Recovery
Advanced • One-Day Instructor-Led Course

For more information contact: info@syntricate.com

The AccessData Password Recovery course provides the knowledge and skills necessary to use PRTK to recover passwords.

Prerequisites:
This course is intended for forensic investigators with a basic working knowledge of the following:
- Forensic Toolkit® (FTK™)
- FTK Imager™
- Password Recovery Toolkit™ (PRTK)
- Microsoft® EFS Encryption
- Basic cryptography

To obtain the maximum benefit from this course, you should meet the following requirements:
- Able to understand course curriculum presented in English
- AccessData BootCamp or equivalent experience with FTK and PRTK
- Previous investigative experience in forensic case work
- Perform basic operations on a personal computer
- Be familiar with the Microsoft Windows environment

Class Materials and Software:
You will receive the associated materials prior to the course.

During this one-day, hands-on course, participants perform the following tasks:
- Review different encryption systems.
- Explore different types of encryption attacks including dictionary, keyspace, and rainbow table attacks.
- Decrypt an ROT13 password.
- Encrypt and decrypt using XOR.
- Decode Trillian passwords.
- Recover extended ASCII character passwords.
- Recover foreign language character set passwords.
- Review what types of information may be gleaned from the suspect to build a custom dictionary for a PRTK attack.
- Review the PRTK interface.
- Define custom dictionaries and attack profiles.
- Decrypt files in PRTK.
- Generate reports to document job results.
- Recover passwords from Microsoft Office products including:
  - Microsoft Word
  - Microsoft Excel
  - Microsoft Outlook
  - Microsoft PowerPoint
  - Microsoft Access
- Recover foreign language passwords.
- Recover a Windows logon password.
- Use the AccessData Decryption Methodology to attack encrypted documents:
  - Export the case index from FTK to build a custom PRTK dictionary.
  - Recover password artifacts from Windows registry files.
  - Build biographical dictionaries using case data and web artifacts.
  - Use the Passphrase Generator to generate possible passphrases from case documents or a dictionary

(Continued on other side)
Module 1: Introduction
Topics:
• Introductions
• Class Materials and Software
• Prerequisites
• Class outline
• Helpful information
Lab:
• Check system information
• Select Windows Explorer display preferences
• Prepare your system

Module 2: Cryptography 101
Objectives:
• Define cryptography and the difficulty levels provided by different algorithms
• List the different types of passwords and standards defined by software applications
• Define cryptography terminology
• Describe the concepts and theory of basic cryptography systems
• Describe symmetric and asymmetric encryption standards
• Describe how digital certificates and signatures are used to encrypt data
Lab:
• Work with data encrypted via ROT 13 and create a key to decrypt the data

Module 3: Decryption Technology - PRTK
Objectives:
• Describe the PRTK/DNA interface
• Utilize the recovery modules
• Import and use dictionaries, rules, and characters to set up an attack profile
• Set up the DNA interface and start a job in DNA
• List the steps to successfully break passwords
• Describe jobs and how to analyze their properties
Lab:
• Review the PRTK interface
• Run a job in PRTK
• Import dictionaries
• Import a golden dictionary
• Decrypt files

Module 4: Lab – Microsoft Decryption Workshop
During this practical, you will reinforce your understanding of encryption models used in Microsoft applications by performing the following tasks:
• Recover extended ASCII passwords
• Recover foreign language character set passwords
• Recover symbol substitution passwords
• Explore ways to exploit cryptographic systems
• Create a concatenation dictionary
• Effectively use PRTK rules and dictionaries for foreign language attacks
• Perform a Windows logon attack
• Perform a PFX attack

Module 5: AccessData Decryption Methodology
Objectives:
• Attack encrypted document using wordlists
• Attack encrypted documents using environment artifacts
• Investigate and uncover suspect intelligence to attack an encrypted document
• Create alternate dictionaries with the AccessData WebCrawler
• Create a passphrase dictionary with the AccessData Passphrase Generator
• Use rainbow tables to break Microsoft Word and Excel Documents

(Continued)