

Applied Decryption

Distributed Network Attack, Password Recovery Toolkit, Forensic Toolkit, Registry Viewer , and FTK Imager

Advanced • Three-day Instructor-led Class



This advanced AccessData training is an intensive, hands-on course that reviews current encryption technology and provides the knowledge and skills necessary to recover passwords using PRTK and DNA.

During this three-day hands-on course, participants perform the following tasks and break / decrypt the listed applications:

Tasks

- Decrypt ROT13 passwords.
- Encrypt and decrypt using XOR.
- Decode Trillian passwords.
- Recover extended ASCII character passwords.
- Recover foreign language character set passwords.
- Recover symbol substitution passwords.
- Break PGP key rings.
- Decrypt virtually encrypted containers.
- Decrypt and hack private keys.
- Decrypt EFS files without using login credentials.
- Use statistical analysis techniques to detect data encrypted using steganography.

Applications

- ARJ
- PGP
- RAR
- Adobe
- WinZip
- Quicken
- CuteFTP
- BestCrypt
- Quickbooks
- VersaCheck
- Microsoft EFS
- Microsoft Money
- Steganography Files
- SAM Logon Passwords
- Microsoft Office Applications

Each day of training includes hands-on labs that require students to apply the concepts covered in class. These performance-based simulations are designed to help participants retain information learned during the training.

Prerequisites

This hands-on course is intended for forensic investigators with experience in forensic case work and a basic working knowledge of FTK, FTK Imager, Registry Viewer, and PRTK.

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

- Attend the AccessData BootCamp or have equivalent experience with FTK, Registry Viewer, and PRTK.
- Have previous investigative experience in forensic case work.

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
- Other forensic training organizations
- Course outline
- Helpful information

Lab

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

Module 2: Cryptography 201

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 the function of digital certificates and signatures.

Lab

- Decrypt ROT13 passwords.
- Encrypt and decrypt using XOR.
- Recover Trillian Passwords.

Module 3: Decryption Technology

Objectives

- Describe the PRTK/DNA interface.
- Utilize the recovery modules.
- Import and use dictionaries, levels, and characters to set up an attack profile.
- List the steps to successfully break passwords.
- Describe jobs and how to analyze their properties.
- Start a job in PRTK.

Lab

- Use PRTK to recover an Arabic password.

Module 4: Working with DNA

Objectives

- Plan and install a DNA network.
- Set up and manage groups of machines.
- Describe the DNA interface and preferences.
- Set up the DNA interface and start a job in DNA.

Lab

- Install DNA.
- Create attack levels.
- Create profiles.

Module 5: Decrypting Selected Applications

During this practical, you will reinforce your understanding of decryption technology by performing the following tasks:

- Recover extended ASCII passwords.
- Recover foreign language character set passwords.
- Recover symbol substitution passwords.
- Explore ways to exploit crypto systems.
- Create a concatenation dictionary.
- Perform analytical, dictionary, and statistical attacks.

Module 6: Working with PGP

During this practical, you will perform the following tasks:

- Implement the web of trust with digital signatures.
- Generate public and private keys in PGP.
- Break PGP key rings.

Module 7: Working with Encrypted Containers

During this practical, you will perform the following tasks:

- Decrypt a virtually encrypted containers.
- Mount the decrypted virtual container.
- Create an image of the mounted virtual container.
- Obtain header information from encrypted containers.

Module 8: Private Keys Revisited

During this practical you will perform the following tasks:

- Export private keys from the Windows environment.
- Decrypt private keys from the Windows environment.
- Hack private keys from the Windows environment.
- Decrypt EFS files without logon credentials.
- Import private keys into your processing environment.

Module 9: Working with Data Within Data

During this practical, you will perform the following tasks:

- Hide data using steganography.
- Identify steganography detection methods.
- Statistically analyze source and carrier files.
- Recover payload from carrier files.

Module 10: AccessData Decryption Methodology

Objectives

- Attack encrypted documents using word lists.
- Attack encrypted documents using environment artifacts.
- Create a biographical profile dictionary using intelligence on the suspect.
- Create a custom dictionary using WebCrawler.
- Create custom dictionary using Passphrase Generator.
- Use Rainbow Tables to decrypt Microsoft Office documents.
- Use NTAccess to manipulate logon credentials.

Lab

- Practically implement the ADM.

Module 11: In Defense of the MD5 Collision

This interactive discussion addresses how to counter an MD5 collision defense. You will review MD5 technology and discuss the MD5 collision potential.

Practical Skills Assessment

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

