Passware Certified Examiner (PCE) Training

Become certified decryption expert

Passware Certified Examiner (PCE) online training is designed to provide computer forensic professionals the knowledge and skills they need to detect, analyze, and decrypt encrypted electronic evidence in the most efficient way. The PCE Training is based on the key capabilities of Passware Kit Forensic.

The Training is accessible during one year from the course start date.

www.passware.com/training

Revision: 20231031

Course Outline:

Session 1: What is Encryption and Decryption?

- Introduction to encryption
- Key terms and definitions
- Types of encryption
- Cryptanalysis

Session 2: Standard Forensic Procedures and Decryption Best Practices

- Forensic procedures
- Decryption best practices

Session 3: Passware Kit Forensic Overview

- Overview of Passware Kit Forensic GUI
- Setting up PKF
- Supported file types and encryption
- PKF for Mac
- Troubleshooting and Support

Session 4: Detecting Encrypted Files

- Introduction to the Passware Encryption Analyzer
- Running a scan
- Interpretation of the results
- Using results

Course Outline:

Session 5: Types of Attacks Available in Passware Kit Forensic

Part1

- Introduction
- Attack options
- Types of attacks
- Attack Settings page
- Grouping and special attacks
- Pausing and resuming attacks

Part 2

- Add and remove attacks
- Combine multiple attacks
- Order attacks
- Save and load attacks models
- Assess and sort attacks by the complexity
- Launch attacks

Session 6: Batch Password Recovery

- Adding files and encryption disk images to the batch mode
- Groups, settings. timeouts, and e-mail notifications
- Running batch password recovery

Course Outline:

Session 7: Dictionary Manager

- Creating and adding a dictionary
- Dictionary Manager
- Password Exchange

Session 8: Hardware Acceleration & Distributed Password Recovery

- What hardware to use
- Distributed password recovery
- Hardware benchmark
- Additional resources

Session 9: Memory Analysis

- Introduction to Volatile Memory (RAM)
- Memory Analysis using PKF
- Passware Bootable Memory Imager (PBMI)
- Performing a Warm-Boot attack

Session 10: Full Disk Encryption

- Supported types of full disk encryption
- Detecting encrypted drives and containers
- Decrypting hard disks

Course Outline:

Session 11: Full Disk Encryption : BitLocker, TrueCrypt, and VeraCrypt

- Decrypting BitLocker drives
- Decrypting TrueCrypt and VeraCrypt volumes

Session 12: Full Disk Encryption : FileVault/APFS Volumes

- Introduction to Apple File Systems and encryption types
- Apple Keychain
- FileVault/APFS volumes decryption and unlock

Session 13: Mobile Device Backups and Apple Keychain

- Mobile devices backups
- Recovering a password for a mobile device backup
- Apple Keychain
- Use cases

Session 14: Resetting a Windows Admin Password

- Creating a bootable drive
- Resetting a password

Course Outline:

Session 15: Standalone System

- Types of passwords located in the registry and user profiles
- Extracting registry files from Windows machines
- Running Passware Kit against SAM
- Windows Hello Sign-in options
- Running Passware Kit against SAM with Windows Hello enabled

Session 16: Hashes

- Hash values and functions
- Rainbow tables
- Salted hashes
- Attacking hashes with Passware Kit
- Supported hash types