Passware

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.

www.passware.com/training

Course Outline:

Session 1: Detecting Encrypted files

- Types of files and encryption able to be detected
- Identifying types of files to decrypt
- Saving and loading Encryption Analyzer search results

Session 2: File Password Recovery

- Types of files supported
- Predefined settings / Wizard

Session 3: Custom dictionary and Keyword lists

- Creating custom dictionary and keyword lists
- Importing those lists to recover passwords
- Password Exchange

Session 4: Types of attacks available in Passware Kit Forensic

- Overview of the various types of attacks, and how they work
- Applying attacks and customizing attack settings

Course Outline:

Session 5: System and GPU Recommendations

- **Hardware acceleration**
  - Supported hardware: GPU Nvidia and AMD cards
  - Supported file types
- **Distributed Password Recovery**
  - Network Setup
  - Windows Agent
  - Linux Agent

Session 6 and 7: Memory Analysis

- Types of encryption-related evidence that could be extracted from a memory image
- How to create the memory image
- How to use hibernation files
- Loading it into Passware Kit Forensic for analysis

Session 8 and 9: Mobile Forensics

- Recover password for encrypted backup
- Recover passwords from iOS keychain
- Recover password for an Android image

Course Outline:

Session 10: Cloud Forensics

- Obtaining the iCloud backup
- Obtaining a OneDrive cloud account

Session 11: Resetting a Windows Admin password

- Creating the bootable USB / CD
- Booting the machine and resetting the password

Session 12: Standalone System

- Recovering passwords from the registry files
- Identifying files required to do the analysis
- How to obtain the registry files

Session 13 and 14: Full Disk Encryption

- Types of Full Disk Encryption
- Choosing between memory analysis and password recovery
- Decrypting various different volumes

Session 15: Completing the Analysis

- A review of best practice procedures
- Exporting the results and saving the details for a report