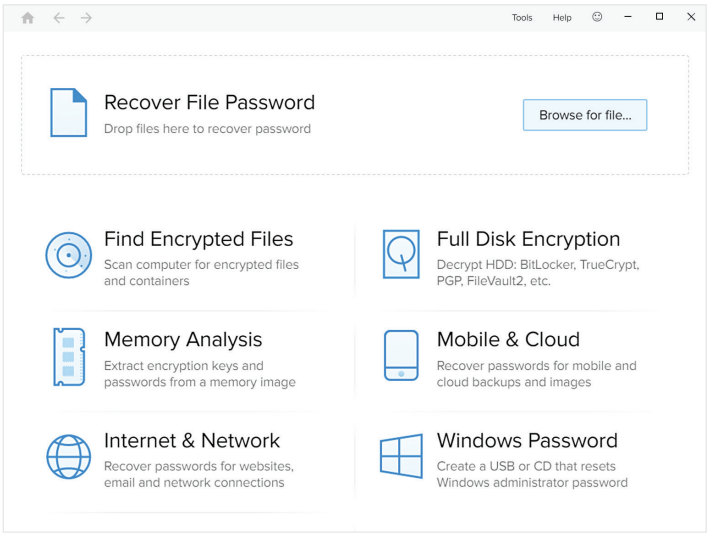
Passware

# PASSWARE KIT FORENSIC

The complete encrypted electronic evidence discovery & decryption solution




## Passware Kit Forensic 2020 v2

Passware Kit Forensic discovers all password-protected items on a computer and decrypts them. The software recognizes 280+ file types and works in batch mode to recover their passwords. Many types of files are decrypted instantly, while other passwords are recovered through Dictionary and Brute-force methods using GPU acceleration and distributed computing (for Windows, Linux, and Amazon EC2). Available for Windows & Mac.

- NEW APFS decryption from Mac with T2
- NEW Mac version BETA
- NEW Passwords extraction from macOS system keychains
- NEW Support for QuickBooks 2020
- NEW Improved GPU performance

## Key Product Features

### Live memory analysis
Analyzes live memory images and hibernation files and extracts encryption keys for hard disks, logins for Windows & Mac accounts, and passwords for files and websites, all in a single streamlined process.

### Cloud data acquisition
Acquires backups and data from cloud services (Apple iCloud, MS OneDrive, and Dropbox). Extracts passwords from iCloud keychains.

### Cross-platform Passware Kit Agents
Supports distributed password recovery with Agents for Windows, Linux, and Amazon EC2.

### 64-bit version
Improved performance, including the capacity to process thousands of files simultaneously and to handle larger dictionary files.

### Automatic updates
Includes automatic software updates with one year of Software Maintenance and Support (SMS) subscription.

### Hardware acceleration
Accelerated password recovery with multiple computers, NVIDIA and AMD GPUs, Decryptum, and Rainbow Tables.

### Mobile forensics
Recovers passwords for Apple iPhone/iPad and Android backups as well as Android images and extracts data from images on Windows phones. Integrated with Oxygen Forensic Suite.

### Password recovery for 280+ file types
MS Office, PDF, Zip and RAR, QuickBooks, FileMaker, Lotus Notes, Bitcoin wallets, password managers, and many other applications.

### Encryption detection and analysis
Detects all encrypted files and hard disk images and reports the type of encryption and the complexity of the decryption.

### Batch processing
Runs password recovery for groups of files without manual intervention.

### Decryption of FDE
Decrypts or recovers passwords for BitLocker, FileVault2, TrueCrypt, VeraCrypt, LUKS, McAfee, APFS, Apple DMG, Symantec, and PGP disk images.

### Password Exchange
Password Exchange provides access to the list of passwords found by Passware Kit users worldwide, offering it as an advanced dictionary to improve chances of finding strong passwords.

**Sales contact**
Phone: +1 (844) 727-7927
E-mail: sales@passware.com

**Passware OÜ**
Kai 1
Tallinn, Estonia, 10111

**Learn more at www.passware.com/pkf**

Passware

# PASSWARE KIT FORENSIC

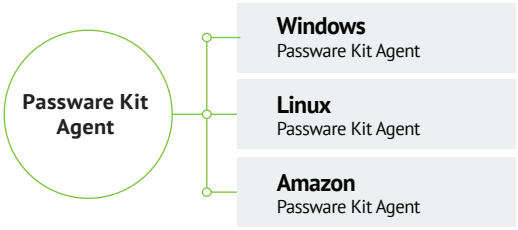
The complete encrypted electronic evidence discovery & decryption solution

## Passware Certified Examiner (PCE) Online Training

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. During the course, students learn how to detect encrypted evidence, recover passwords for all common file types, analyze memory images, recover passwords for mobile backups, decrypt hard drives, and more. The course consists of 15 short video sessions. Participants in this training course may take the exam to receive a Passware Certified Examiner (PCE) designation. Learn more at **passware.com/training**

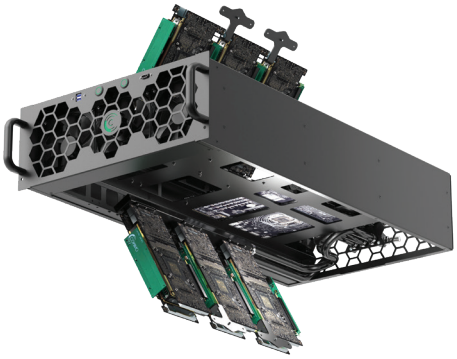
## Network Distributed Password Recovery: Passware Kit Agent

Passware Kit Agent is a network distributed password recovery worker for Passware Kit Forensic. It runs on Windows and Linux, 64- and 32-bit, has linear performance scalability. Each computer running Passware Kit Agent supports multiple CPUs, GPUs, and TPR accelerators simultaneously. Passware Kit Forensic comes with 5 agents included with ability to purchase more separately as needed. Learn more at **passware.com/distributed**




## Hardware Acceleration of Password Recovery Attacks

Passware Kit Forensic can increase password recovery speed up to 400 times by using a single GPU (Graphics Processing Unit) card, and up to 12,000 times by using a single Decryptum PR 2080TI-S/12 4U unit. Distribute password recovery tasks over a network of Windows or Linux computers, as well as Amazon EC2, for linear scalability. For even higher performance use Decryptum, our ultra-compact liquid-cooled GPU accelerated devices - world's fastest scalable turn-key decryption solution for password recovery. Learn more at **decryptum.com**



| File Type | Encryption | CPU Speed<br>i5-4570 | NVIDIA Speed<br>RTX 2080 Ti | Decryptum<br>PR 2080TI-S/12 4U |
|---|---|---|---|---|
| MS Office 2013+ | AES-256 | 78 | 23,458 | 285,000 |
| RAR 5.x | AES-256 | 98 | 91,542 | 1,205,000 |
| macOS / FileVault2 / APFS | AES-256 | 53 | 17,207 | 210,000 |
| Apple iTunes Backup / iOS 10.x+ | AES-256 | <1 | 307 | 4,000 |
| MS Windows / BitLocker | BitLocker | 7 | 3,000 | 40,000 |

(passwords/second)

**Sales contact**
Phone: +1 (844) 727-7927
E-mail: sales@passware.com

**Passware OÜ**
Kai 1
Tallinn, Estonia, 10111

**Learn more at www.passware.com/pkf**