**Passware Kit Forensic 2021 v4**

Passware Kit Forensic discovers all password-protected items on a computer and decrypts them. The software recognizes 300+ 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** Batch mode for FDE decryption
- **NEW** Email notifications for password recovery jobs
- **NEW** Support for AFF4 images
- **NEW** FileMaker 19
- **NEW** Turkish dictionary
- **NEW** Dark theme
- **NEW** Usability improvements

**Key Product Features**

**Live Memory Analysis**
Analyze 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.

**Email Notifications**
Automatically sends an email whenever a password is found or the recovery process gets finished.

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

**Passware Bootable Memory Imager**
A UEFI compatible tool that acquires memory images of Windows, Linux, and Mac computers. Passware Memory Imager works with Windows computers that have Secure Boot enabled.

**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.

**Password Recovery for 300+ 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 and FDE images without user intervention.

**Decryption of FDE**
Decrypts or recovers passwords for APFS, Apple DMG, BitLocker, Dell, FileVault2, LUKS, McAfee, PGP, Symantec, TrueCrypt, and VeraCrypt 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.
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. Distribute password recovery tasks over a network of Windows or Linux computers, as well as Amazon EC2, for linear scalability.

<table>
<thead>
<tr>
<th>File Type</th>
<th>Encryption</th>
<th>CPU Speed</th>
<th>NVIDIA Speed</th>
<th>AMD Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS Office 2013+</td>
<td>AES-256</td>
<td>78</td>
<td>28,557</td>
<td>23,883</td>
</tr>
<tr>
<td>RAR 5.x</td>
<td>AES-256</td>
<td>98</td>
<td>114,597</td>
<td>117,867</td>
</tr>
<tr>
<td>macOS / FileVault2 / APFS</td>
<td>AES-256</td>
<td>53</td>
<td>65,588</td>
<td>65,392</td>
</tr>
<tr>
<td>Apple iTunes Backup / iOS 10.x+</td>
<td>AES-256</td>
<td>&lt;1</td>
<td>372</td>
<td>361</td>
</tr>
<tr>
<td>MS Windows / BitLocker</td>
<td>BitLocker</td>
<td>7</td>
<td>3,947</td>
<td>3,623</td>
</tr>
</tbody>
</table>

Encryptions: AES-256, BitLocker
(Passwords/Second)

*Passware* and Passware logo are trademarks of Passware. All other names mentioned are trademarks, registered trademarks or service marks of their respective owners.