PASSWARE KIT FORENSIC

The complete encrypted electronic evidence discovery & decryption solution

Passware Kit Forensic 2020 v1

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).

- Dictionary Manager
- Support for VeraCrypt GPT
- Faster memory image analysis for VeraCrypt
- Instant BitLocker decryption with a known VMK
- Extraction of FileVault2 password hint and recovery key
- Passwords extraction from Windows Hello standalone systems

**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**
Accelerates password recovery with multiple computers, NVIDIA & AMD GPUs, TPR, and Rainbow Tables.

**Mobile forensics**
Recover 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.

**Learn more at www.passware.com/pkf**
PASSWARE KIT FORENSIC
The complete encrypted electronic evidence discovery & decryption solution

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.

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 3,200 times by using 8 GPUs in a single computer. 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 i5-4570</th>
<th>NVIDIA Speed RTX 2080 Ti</th>
<th>AMD Speed R9 Fury</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS Office 2013 and higher</td>
<td>AES-256</td>
<td>78</td>
<td>19,335</td>
<td>4,390</td>
</tr>
<tr>
<td>TrueCrypt</td>
<td>System (1-cascade)</td>
<td>591</td>
<td>1,050,000</td>
<td>337,650</td>
</tr>
<tr>
<td>RAR5</td>
<td>AES-256</td>
<td>98</td>
<td>80,893</td>
<td>25,700</td>
</tr>
<tr>
<td>iTunes Backup v9</td>
<td>AES-256</td>
<td>2,006</td>
<td>280,000</td>
<td>91,400</td>
</tr>
<tr>
<td>BitLocker</td>
<td>BitLocker</td>
<td>7</td>
<td>2,566</td>
<td>818</td>
</tr>
</tbody>
</table>

(passwords/second)