# Passware

Passware Kit Forensic

The complete encrypted electronic evidence discovery & decryption solution

What's new in 2022 v3

- Deleted data recovery for APFS
- Decryption of QuickBooks for Mac 2022
- GPU acceleration for bcrypt hashes
- Enhanced support for Acronis
- Password recovery for Dashlane for Mac
- Hybrid rainbow tables support

For the full list of features & updates visit **passware.com/pkf**
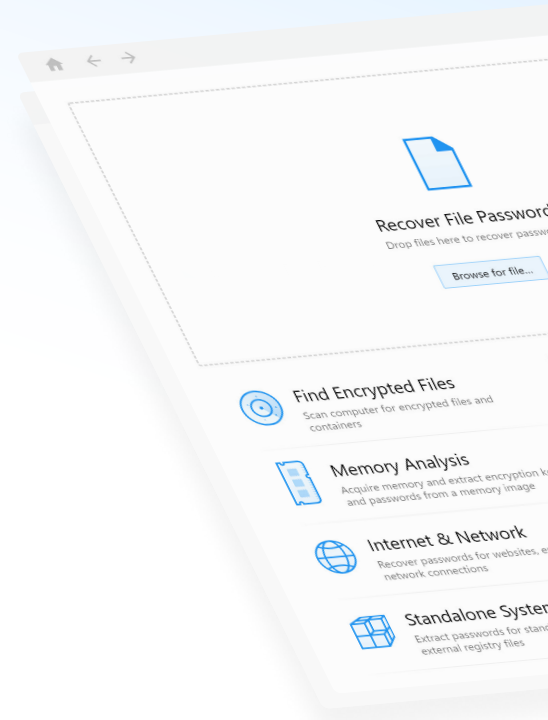
Live memory analysis

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.

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.

Hardware acceleration

Accelerated password recovery with multiple computers, NVIDIA and AMD GPUs, 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.

Decryption of FDE

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

Batch processing

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.

Request a free trial

Rev. 20220725

Passware Certified Examiner (PCE) Online Training

Designed specifically for computer forensic professionals, this self-paced course provides world-class knowledge and skills to analyze and decrypt encrypted electronic evidence in an easy to follow format. 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. Sign up 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**

Passware T2 Add-on

Passware Kit Forensic T2 Add-on is an advanced forensic solution that allows users to recover passwords and decrypt disks for Macs with Apple T2 Security Chips. Passware Kit Forensic T2 Add-on is available for law enforcement and other types of government organizations and private companies with justifiable business needs, such as forensic firms or corporate investigation teams. All orders are subject to manual verification.

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. Mac version supports OpenCL acceleration on AMD GPU and NVIDIA/AMD eGPU. Distribute password recovery tasks over a network of Windows or Linux computers, as well as Amazon EC2, for linear scalability.

File Type	Encryption	CPU Speed i5-4570	NVIDIA Speed GeForce RTX 3090	AMD Speed Radeon RX 6900 XT
MS Office 2013+	AES-256	78	28,557	23,883
RAR 5.x	AES-256	98	114,597	117,867
macOS / FileVault2 / APFS	AES-256	53	65,588	65,392
Apple iTunes Backup / iOS 10.x+	AES-256	<1	372	361
MS Windows / BitLocker	BitLocker	7	3,947	3,623

(passwords/second)