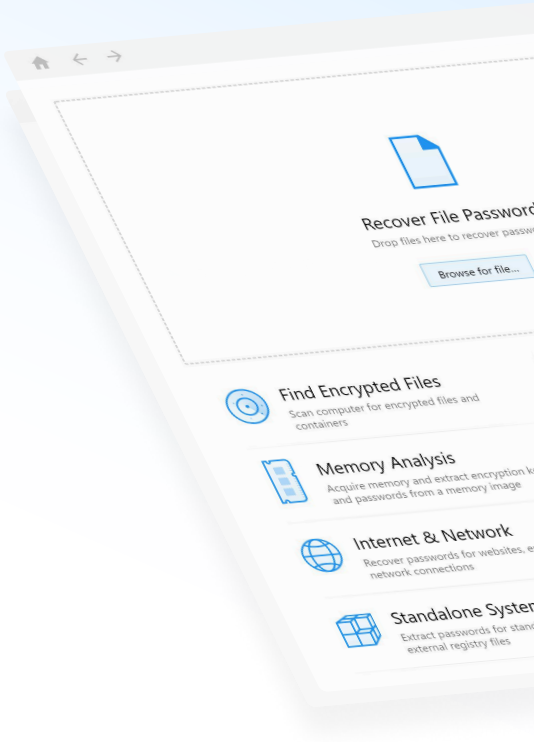
Passware

Passware Kit Forensic

The complete encrypted electronic evidence discovery and decryption solution.



What's new in 2026 v4

- Decryption of eCryptfs
- Saving decrypted images in E01 format
- Password recovery for iWork 2026 files
- Extended support for VeraCrypt Portable
- Compatibility with macOS 27 Golden Gate

For the complete list of features and updates, visit **passwa.re/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, Amazon EC2, and Microsoft Azure. Resource Manager sets up password recovery clusters and manages local and remote hardware.

Hardware acceleration

Accelerated password recovery with multiple computers, NVIDIA, AMD, and Intel Arc GPUs, and Rainbow Tables. Caches previously tested passwords to eliminate redundant checks and improve the overall password recovery performance.

Automatic updates

First year of automatic updates included. For Perpetual licenses, it is possible to renew the annual Software Maintenance and Support (SMS) subscription.

Password recovery for 420+ file types

MS Office, PDF, Zip and RAR, QuickBooks, FileMaker, Lotus Notes, Apple 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 and containers

Decrypts or recovers passwords for APFS, Apple DMG, BitLocker, Dell, eCryptfs, FileVault2, LUKS, McAfee, PGP, SanDisk, Steganos, Symantec, TrueCrypt, VeraCrypt containers, disk images, folders, and vaults.

Batch processing

Runs password recovery for groups of files and FDE images without user intervention. Fast transferring of the password recovery process to another computer using digests instead of large files or disk images. Automatic check of the recovered passwords for previous and skipped files in a session.

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.

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

Passware, Inc.
800 West El Camino Real, Suite 180
Mountain View, CA 94040, USA

Passware OÜ
Jõesuu 6-8
Tallinn, Estonia, 11911

Passware

Rev. 20261020

Passware

Passware Certified Examiner (PCE) Online Training

Passware CERTIFIED EXAMINER

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

Azure Agents · Amazon Agents · Windows Agents · Linux Agents

Passware Kit Agent is a network distributed password recovery worker for Passware Kit Forensic. It runs on Windows and Linux, 64- and 32-bit, and has linear performance scalability. Each computer running Passware Kit Agent simultaneously supports multiple CPUs and GPUs. Users can remotely control all the Agents within their network directly from the PKF. Passware Kit Forensic comes with 5 agents with the ability to purchase more separately as needed. Learn more at **passware.com/distributed**

Optional Device Decryption Add-on

T2 · TPM · Lenovo

Exclusive forensic solution that allows users to unlock, decrypt, and recover passwords or recovery keys for:

- BitLocker-encrypted devices with TPM, incl. PIN protection
- Macs with Apple T2 Security Chip
- External HDDs: Western Digital My Passport (2014–2024), My Book 4TB/6TB (2021–2024), Transcend SSDs, Seagate, LaCie

Hardware Acceleration and Resource Management

Passware Kit Forensic can increase password recovery speed up to 1,200 times by using a single GPU (Graphics Processing Unit) card. Mac version supports OpenCL acceleration on AMD GPU and NVIDIA/AMD/Intel Arc eGPU. Distribute password recovery tasks over a network of Windows or Linux computers, as well as Amazon EC2 and Microsoft Azure, for linear scalability. Set up the password recovery cluster easily with the built-in Resource Manager. Smart resource allocation algorithm for concurrent file processing minimizes hardware idle time.

File Type	Encryption	Intel CPU i7-9700F	NVIDIA GeForce RTX 4090	AMD Radeon RX 6900 XT	Intel Arc B580
MS Office 2013+	AES-256	78	48,581	23,883	5,139
RAR 5.x	AES-256	98	201,723	117,867	67,707
macOS / FileVault2 / APFS	AES-256	53	117,395	65,392	41,221
Apple iTunes Backup / iOS 10.x+	AES-256	<1	831	361	18
MS Windows / BitLocker	BitLocker	7	7,312	3,623	2,114

View complete hardware benchmark: **passwa.re/benchmark** (recovery speed in passwords per second)

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

Passware, Inc.
800 West El Camino Real, Suite 180
Mountain View, CA 94040, USA

Passware OÜ
Jõesuu 6-8
Tallinn, Estonia, 11911

Passware

Rev. 20261020