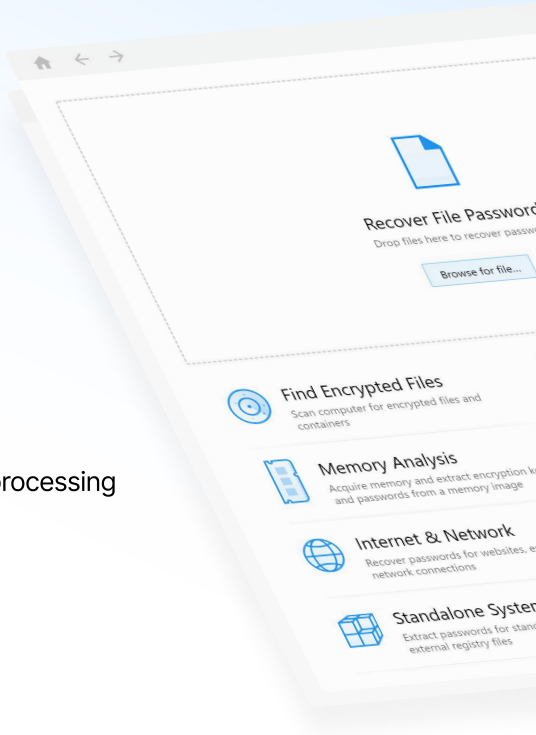
Passware

Passware Kit Forensic

The complete encrypted electronic evidence discovery and decryption solution.



What's new in 2025 v2

- Password recovery for VeraCrypt volumes with BLAKE2s-256 encryption
- VeraCrypt memory analysis: support for hidden OS for latest versions and faster processing
- Smart resource allocation algorithm for distributed and batch processes
- Password recovery for individual Apple Notes
- Password recovery for Bitcoin Core wallet v.20 and higher
- Password recovery for WinRAR v.7 and RAR hashes

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.

Password recovery for 380+ file types

MS Office, PDF, Zip and RAR, QuickBooks, FileMaker, Lotus Notes, Apple Notes, Bitcoin wallets, password managers, and many other applications.

Email notifications

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

Encryption detection and analysis

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

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.

Decryption of FDE

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

Hardware acceleration

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

Batch processing

Runs password recovery for groups of files and FDE images without user intervention.

Automatic updates

Optional automatic software and agents updates with one year of Software Maintenance and Support (SMS) subscription. First year of SMS included.

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. 20250403

Passware

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**

Passware CERTIFIED EXAMINER

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, 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**

Windows Agents

Linux Agents

Azure Agents

Amazon Agents

Optional Device Decryption Add-on

Passware Kit Device Decryption Add-on is an advanced forensic tool that allows users to unlock, decrypt, and recover passwords or recovery keys for: Western Digital My Passport 2014–2024 and My Book 2021–2024 4TB/6TB, Seagate and LaCie disks, as well as Lenovo ThinkPads and Macs with Apple T2 Security Chips. The 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.

T2 WD Lenovo

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 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	CPU Speed i7-9700F	NVIDIA Speed GeForce RTX 4090	AMD Speed Radeon RX 6900 XT
MS Office 2013+	AES-256	78	48,581	23,883
RAR 5.x	AES-256	98	201,723	117,867
macOS / FileVault2 / APFS	AES-256	53	117,395	65,392
Apple iTunes Backup / iOS 10.x+	AES-256	<1	831	361
MS Windows / BitLocker	BitLocker	7	7,312	3,623

(passwords/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