

PASSWARE KIT FORENSIC

The complete encrypted electronic evidence discovery & decryption solution



Passware Kit Forensic 2019 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 (both for Windows and Linux).

- NEW** Password Exchange
- NEW** GPU monitoring
- NEW** Easy access to Passware Kit Agent logs
- NEW** Instant decryption of TrueCrypt hidden partitions
- NEW** Decryption of macOS Mojave APFS disks
- NEW** Additional dictionaries

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).

Passware Kit Agent for Linux

The Linux version can run a portable Passware Kit Agent from a bootable Linux USB drive on any system without installation.

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

Recovers 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, and many other popular 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.

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 for linear scalability.

File Type	Encryption	CPU Speed	NVIDIA Speed	AMD Speed
MS Office 2013 and higher	AES-256	78	10,378	5,157
TrueCrypt	System (1-cascade)	591	565,823	300,463
RAR5	AES-256	98	47,329	31,303
iTunes Backup	AES-256	2,006	153,978	92,467
BitLocker	BitLocker	7	1,481	836

(passwords/second)