Passware

Password Recovery Kit Forensic 13.0

All-in-one password recovery and encrypted evidence discovery solution

Passware Kit Forensic helps investigators to discover encrypted electronic evidence and decrypt it quickly. This software combines fast encryption detection engine, password recovery modules for 200+ file types, batch processing, and a portable version to meet all the requirements of law enforcement, governmental agencies, as well as corporate forensic professionals.

The tool cracks passwords for documents, archives, databases and hard drives, Windows and Mac users, email accounts and websites. Many types of passwords are recovered or reset instantly.

To achieve the highest speed, Passware Kit Forensic uses distributed password recovery and cloud computing, NVIDIA and ATI GPU hardware acceleration. Multiple files are processed simultaneously.

Passware Kit Forensic is the only commercial software capable of instant decryption of BitLocker, TrueCrypt, FileVault2, and PGP hard disks, MS Office 2013 documents, as well as instant recovery of passwords for websites, Windows and Mac users, by analyzing hibernation files and live memory images acquired via FireWire.
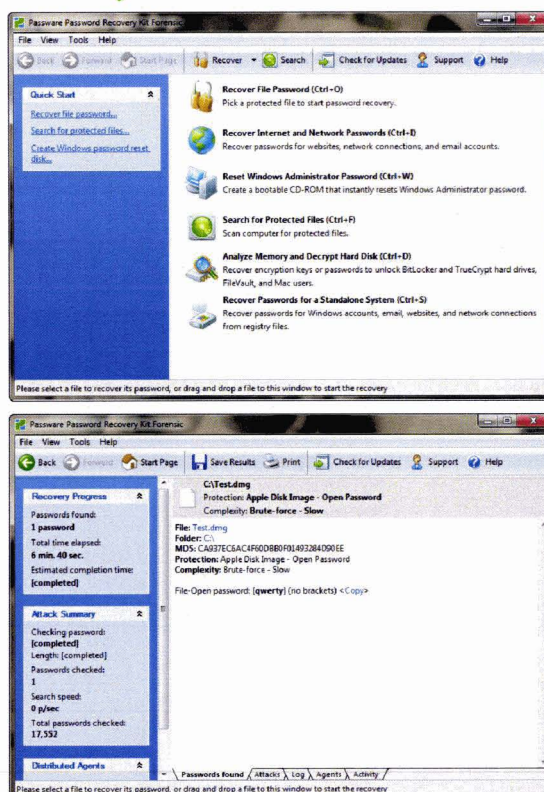
Key Benefits

64-bit version New
Improved performance while processing thousands of files simultaneously and larger dictionary files

Recovers passwords for 200+ file types Updated
Including MS Office, PDF, Zip & RAR, QuickBooks, FileMaker, Lotus Notes, and many other popular applications

Batch processing
Runs password recovery for groups of files without manual intervention

Scans computers for encrypted evidence
Detects all the encrypted files and hard disk images, reports encryption type and decryption complexity

Live Memory Analysis
Acquires live memory image over FireWire, analyzes it, and extracts encryption keys for BitLocker, TrueCrypt, PGP, MS Office files, as well as passwords for websites, Windows and Mac users

Decrypts FDE: BitLocker, TrueCrypt, FileVault2, and PGP
Instantly decrypts hard disk images with live memory analysis or recovers their passwords with accelerated brute-force attacks

Accelerated password recovery: GPU, TACC, Distributed Computing, Rainbow Tables Updated
Uses the power of multiple computers (5 Passware Kit Agents included), improves password recovery speed with NVIDIA and ATI GPU cards, Tableau TACC, and Rainbow Tables

Integrated with Guidance EnCase v7
One-click password recovery directly from EnCase

Passware Kit Forensic offers support for:

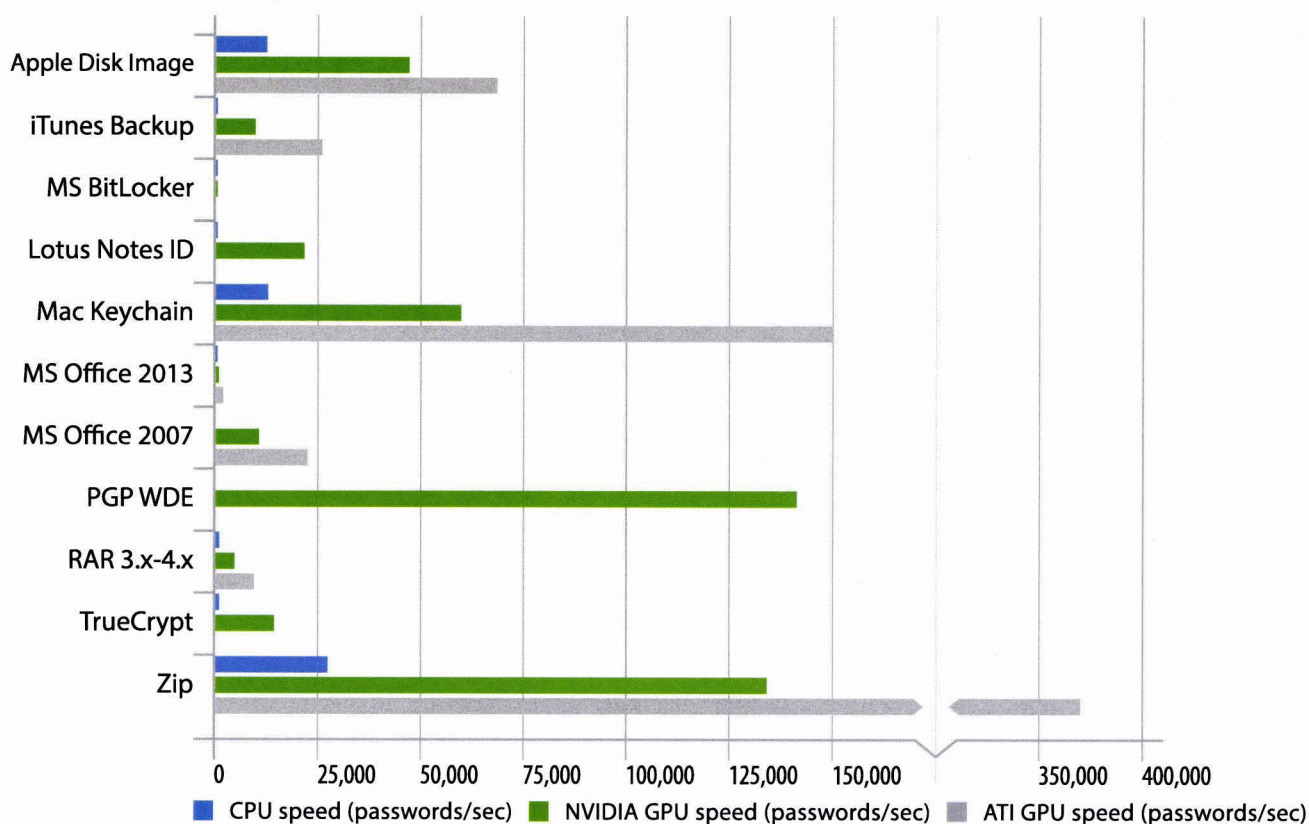| Documents & Databases	Hard Disk Encryption	Email Accounts and Web Browsers
MS Excel (XLSX) ▯ ⬆, (XLS) ⚡	BitLocker ▯ ⬆	Google Chrome ⚡ ▯
MS Word (DOCX) ▯ ⬆, (DOC) ⚡	TrueCrypt ▯ ⬆	Mozilla Firefox ⚡ ▯
Adobe Acrobat (PDF)	FileVault2 ▯	Internet Explorer ⚡ ▯
Lotus Notes (ID) ⬆	PGP WDE ▯ ⬆	MS Outlook ⚡
MS Access (ACCDB) ⬆, (MDB) ⚡	PGP ⬆	Safari ⚡ ▯
MS SQL (MDF) ⚡	Apple Disk Image ⬆	
MS Office VBA ⚡		

Mobile	Financial Software	Archives	User Login Accounts
iTunes backup (PLIST) ⬆	QuickBooks (QBW, QBA) ⚡	Zip (ZIP) ⬆	Windows ▯ ⚡
Android backup ⬆	Quicken (QDF) ⚡	RAR ⬆	Mac OS X ▯
	ACT! (ADF) ⚡	7-Zip (7Z) ⬆	

and 50 other file types.

⚡ – instant password recovery or decryption; ▯ – instant decryption possible with live memory analysis;

⬆ – hardware acceleration supported for brute-force password recovery processes.

Password recovery speeds

■ CPU speed (passwords/sec) ■ NVIDIA GPU speed (passwords/sec) ■ ATI GPU speed (passwords/sec)